CHINTHURST SCHOOL

TRADITIONAL VALUES | MODERN TEACHING

Chinthurst Preparatory School

E-Safety Policy

This policy fully incorporates the recommendations of 'Keeping Children Safe in Education' as published by the Department for Education – September 2016

Reviewed by TB/SN/WB - September 2016

Next review date – September 2017

Contents

Communication of Policy

4.1 Pupils

4.2 Staff

4.3 Parents

4.4 Process of incident handling

4.5 E-Safety rules

4.6 Acceptable Use Agreement

4.7 Staff Information Systems Code of Conduct

1.1- School E-Safety Policy

1.1.1 - E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology.

1.1.2 - It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

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

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

Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the school's ISP including the effective management of content filtering.
- National Education Network standards and specifications.

1.1.5 - Date of latest update: April 2016
The E-Safety coordinator approved the policy in: April 2016
Policy is available for staff and parents at the school and http://chinthurstschool.co.uk/policies.

1.1.6 - Considerations made by the school as part of this policy:

- The Designated Safeguarding Leads (DSL's) are: Tim Button and Maria Panayi.
- The E-Safety Coordinator is: Will Beadle
- Technical advice/support regarding E-Safety matters is supplied by '*Brandtek IT Services Ltd'*.
- Has e-safety training been provided for both pupils and staff: Yes, Staff INSET / Pupils Spring 2016
- Do all staff sign and acknowledge an ICT Code of Conduct on appointment? Yes
- Do parents sign and return an agreement that their child will comply with the School e-Safety Rules? Yes
- Have school e-Safety Rules been set for pupils? Yes
- Are these Rules displayed in all rooms with computers used by children? Yes
- Has the school filtering policy has been approved by SMT? Yes
- Has an e-Safety Coordinator received training in accordance with the NSPCC and CEOP? Yes

1.1.7 - The school has appointed an e-Safety coordinator. Our e-Safety Policy has been written by the school. It has been agreed by the senior management team and approved by governors. The e-Safety Policy will be reviewed annually. This policy will next be reviewed September 2016.

1.2 - Why is Internet Use Important?

1.2.1 - 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 information and administration systems.

1.2.2 - Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction.

1.2.3 - Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

1.2.4 - Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

1.3 - How does Internet Use Benefit Education?

1.3.1 - Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries.
- Inclusion in the National Education Network, which connects all UK schools.
- Educational and cultural exchanges between pupils world-wide.
- 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 support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.

1.4 - How can Internet Use Enhance Learning?

1.4.1 - The School Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.

1.4.2 - Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

1.4.3 - Internet access will be planned to enrich and extend learning activities.

1.4.4 - Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.

1.4.5 - Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.1 - Authorised Internet Access

2.1.1 - The School will maintain a current record of all staff and pupils who are granted Internet access.

2.1.2 - All staff must read and adhere to the school code of conduct before using any school ICT resource.

2.1.3 - Parents will be informed that pupils will be provided with supervised Internet access.

2.1.4 - Parents will be asked to sign and return a consent form for pupil access.

2.2 - World Wide Web

2.2.1 - If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to network manager via the e-safety coordinator.

2.2.2 - School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

2.2.3 - Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

2.3 – Email

2.3.1 - Pupils may only use approved e-mail accounts on the school system.

2.3.2 - Pupils must immediately tell a teacher if they receive offensive e-mail.

2.3.3 - Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

2.3.4 - Access in school to external personal e-mail accounts may be blocked.

2.3.5 - E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

2.3.6 - The forwarding of chain letters is not permitted.

2.4 - Social Networking

2.4.1 - School blocks/filters access to social networking sites and newsgroups unless a specific use is approved.

2.4.2 - Pupils will be advised never to give out personal details of any kind, which may identify them or their location.

2.4.3 - Pupils should be advised not to place personal photos on any social network space.

2.4.4 - Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

3.1 - Cyber Bullying

3.1.1 - School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyber bullying and should work together to create an environment in which pupils can learn and develop and staff can have fulfilling careers free from harassment and bullying. ***(DfE; Cyber bullying: 2014)***.

3.1.2 - What is Cyber Bullying?

"Cyber bullying is similar to other types of bullying, except it takes place online and through text messages sent to cell phones. Cyberbullies can be classmates, online acquaintances, and even anonymous users, but most often they do know their victims" ***(NCPC; Cyber Bullying)***.

3.1.3 - Forms of Cyber Bullying

- There are various forms of cyber bullying, most commonly involving the use of online materials, programmes and resources, whilst also including the use of messaging. This can include both computer-generated and telephone-based text messages.

- Other forms of Cyber Bullying can take place via differing social media platforms. These websites allow an ease of access in terms of messaging/sharing information across a multitude of differing aspects.

- Further forms of cyber bullying can include:

Sending someone mean or threatening emails, instant messages, or text messages.
Excluding someone from an instant messenger buddy list or blocking their email for no reason.
Tricking someone into revealing personal or embarrassing information and sending it to others.
Breaking into someone's email or instant message account to send cruel or untrue messages while posing as that person.
Creating websites to make fun of another person such as a classmate or teacher. ***(NCPC; Cyber Bullying)***

3.1.4 - Signs and Symptoms

The signs and symptoms of someone being bullied/bullying is taking place are outlined in full detail as per our "Anti-Bullying" policy; Section 1.5: *Signs and Symptoms.* A link to which can be found here: http://chinthurstschool.co.uk/docs/2016%20Policies%20/Anti-Bullying%20Policy%20v2.pdf.

3.1.5 - What to do if Cyber Bullying is suspected

If cyber bulling is suspected, the procedure to be followed is that which is outlined as per our "Anti-Bullying" policy; Section 1.8: *The procedure to follow at Chinthurst School.* A link to which can be found here: http://chinthurstschool.co.uk/docs/2016%20Policies%20/Anti-Bullying%20Policy%20v2.pdf.

The "*Reporting Bullying Pro-Forma"* – Appendix 1 (*Chinthurst School Anti-Bullying Policy*), will be used to effectively record any and all cyber bullying incidents as outlined in the procedures above.

3.2 - Filtering

3.2.1 - The school will ensure filtering systems are as effective as possible.

3.3 - Managing Emerging Technologies

3.3.1 - Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.3.2 - Mobile phones will not be used for personal use during lessons or formal school time.

3.3.3 - The sending of abusive or inappropriate text messages is strictly forbidden.

3.4 - Published Content and the School Web Site

3.4.1 - The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

3.4.2 - The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.5 - Publishing Pupils' Images and Work

3.5.1 - Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

3.5.2 - Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

3.5.3 - Work can only be published with the permission of the pupil and parents.

3.6 - Information System Security

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

3.6.2 - Virus protection will be installed and updated regularly.

3.7 - Protecting Personal Data

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

3.8 - Assessing Risks

3.8.1 - The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

3.8.2 - Neither the school nor external service providers can accept liability for the material accessed, or any consequences of Internet access.

3.8.3 - 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.

3.9 - Handling e-safety Complaints

3.9.1 - Complaints of Internet misuse will be dealt with by a senior member of staff.

3.9.2 - Any complaint about staff misuse must be referred to the head teacher.

3.9.3 - Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

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

3.9.5 - Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

3.10 - Procedure and Recording of E-Safety incidents

3.10.1 - Any incidents concerning the safe use of technology, such as a breach of the filtering system or other inappropriate activity will be logged in the school's e-safety log. This log will be used in conjunction with providing further e-safety and security measures, whilst endeavouring to continually improve, update and further develop our differing policies and filtering systems.

3.11.2 - However, any 'cyber' bullying incidents will be dealt with separately, in alignment with alternate forms of bullying. This will therefore be utilising the procedure and indeed the pro-forma exampled as per the Anti-Bullying policy; Section 1.8: *The procedure to follow at Chinthurst School*. A link to which can be found here: http://chinthurstschool.co.uk/docs/2016%20Policies%20/Anti-Bullying%20Policy%20v2.pdf.

4.1 – Pupils

4.1.1 - Rules for Internet access will be posted in all networked rooms.

4.1.2 - Pupils will be informed that Internet use will be monitored.

4.2 – Staff

4.2.1 - All staff will be given the School e-Safety Policy and its importance explained.

4.2.2 - Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

4.3 – Parents

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

4.4 - Process of incident handling

4.4.1 - Pupil:
Review incident and decide on appropriate course of action, applying sanctions as necessary.

4.4.2 - Staff:
Review incident and decide on appropriate course of action, applying sanctions as necessary.

4.5 - Pupil e-safety rules

4.5.1 - *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.

4.5.2 - *Key Stage 2*

- Think then Click
- We ask permission before using the Internet.
- Think carefully about which websites you use.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open e-mails sent by anyone we don't know.
- We do not talk to anyone over the Internet who we don't know.

4.5.3 - 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 ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes are not permitted.

4.5.4 - The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail 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 for storing unauthorised or unlawful text, imagery or sound.

4.6 - Acceptable Use Agreement

4.6.1 - All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign a document to show that the e-Safety Rules have been understood and agreed within the Home –School Agreement.

4.7 - Staff Information Systems Code of Conduct

4.7.1 - To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to read this code of conduct and sign to acknowledge having done so:

- 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.
- I understand that 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 I will not disclose any password or security information to anyone other than an 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 Coordinator.
- I will ensure that any electronic communications with pupils 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 e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.