CHARD SCHOOL

E-SAFETY POLICY

Chard School pupils are growing up in a digital age where the internet provides them with a world of opportunities to learn, communicate and express themselves. The internet can be a wonderful resource for education and personal development. We fully recognise the contribution technology can make to children in school.

The aim of this policy is to safeguard and promote our pupils' safe use of internet and electronic communication technology. The policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

The policy provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

The policy aims to protect pupils and staff from the adverse effects of electronic communication which may include:

- Cyberbullying
- Receiving or publishing inappropriate content
- Grooming
- Requests for personal information
- Publishing personal information
- Identity theft
- Corruption or misuse of data
- Online gambling
- Sexting
- Pornography
- Hacking and security breaches

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils
- A comprehensive, agreed and implemented E-Safety Policy
- Secure, filtered broadband
- A school network that is compliant with National Education Network standards and specifications

Chard School takes e-safety seriously:

- The school works in partnership with ICT contractors to ensure that filtering systems are as effective as possible. Any breaches should be reported for local blocking.
- Virus protection for the whole network is installed and updated regularly.
- Rules for internet access and use are displayed in the ICT room.
- Complaints of internet misuse by pupils are investigated by the school.
- Concerns about staff misuse are referred to the Head.
- The IT consultants employed by the school review system security on a regular basis.

- Chard School will audit ICT use on a regular basis to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective through informal/formal monitoring.

Internet use enhancing learning

- The school internet access is designed expressly for pupil use.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use through discussion and signing of the Pupil Acceptable User Policy (AUP) on an annual basis.
- 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 shown how to publish and present information to a wider audience and how to evaluate internet content.
- The school will ensure internet derived material complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy and how to report unpleasant internet content.

School Staff E-Safety

All staff must adhere to the policies and procedures relating to use of the network and mobile devices and will read and sign the Acceptable User Policy (AUP) before using any school ICT resources.

The school can monitor both e'mail and internet use to help ensure that it is being used legitimately. Teaching staff should take responsibility for checking that filtering is up to date and appropriate for their lessons. Given the potential dangers of contacting pupils via social network sites and private e'mails, staff should not use these means of communication in or out of school. Staff should not be "friends" with any pupil who is in the school nor should they allow pupils to access their "wall". Staff are reminded that they are required to remain professional and confidential about school matters and these should not be discussed in open forums or on social networking sites.

Pupil E-Safety

Parents/guardians will be asked to sign the Pupil Acceptable User Policy (PAUP) for their child to use the school ICT resources.

The pupils have supervised access to the internet. The ICT room is only accessible when a teacher is present. Pupils should understand that the use of the school network is a privilege which can be removed in the case of misuse. The school Wi-Fi code is never to be given to pupils.

Pupils are not allowed to access social networking sites from school and the school is vigilant in ensuring that access through proxy sites is not allowed.

Some pupils may inadvertently or deliberately access unsuitable sites which contain violent, pornographic or harmful images even on the school network with its controls and filters. Children will be closely supervised when using the internet as it cannot be guaranteed that any filtering system is completely reliable.

If unsuitable material is accessed then staff should take immediate action by closing or minimising the window. The incident should be reported to the Head for investigation.

Pupils who have been upset or disturbed in any way by what they have seen should be reassured by the member of staff.

E-Safety training will be embedded within the ICT scheme of work and the PSHE (Personal, Social and Health Education) curriculum.

Pupils are not allowed personal electronic devices such as mobile phones, laptops, iPads, and E-readers at school at any time.

Community E-Safety

Any person not directly employed by the school will be asked to read and accept the Staff/Governor/Visitor Acceptable User Policy before being allowed to access the internet from the school site.

All users of the school computer system understand that the systems in place afford no privacy.

Use and storage of images generated in the school

Parents are invited to agree to the school using anonymous photographs of their children which may be published in the prospectus or on the website. Parents indicate this consent on the form which is sent out annually for this purpose. Chard School will make every effort to ensure that children whose parents/guardians have refused permission for images of their children to be used are excluded from any event in which the media are present or prevent them from being photographed. We will always complain to the Press Complaint Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people.

Photographs are taken extensively of pupils in the EYFS to provide evidence of their achievements. These photographic records will only be shown to the parents and staff. EYFS staff may not use their own personal phones, laptops, iPads or other to capture images of pupils. Only school owned equipment may be used for this purpose.

Cameras or other recording devices must never be used whilst changing a child or in the games changing rooms. To avoid allegations, such devices must be switched off before entering the room or left outside the room. In the EYFS setting, personal devices are secured in a locked cabinet and not used during a session.

Chard School only uses images of pupils for the following:

- Internal displays within the school premises
- Communications with the school community (parents, pupils, staff, Governors and Old Cerdics)
- Marketing the school both digitally by website, prospectus, displays at educational fairs and other marketing functions, and by other means
- As evidence of attainment when required by external awarding bodies
- Informing parents of the activities of their own child

A school digital camera is provided and all images should only be downloaded onto the school network. The school camera should be used wherever possible in preference to a device belonging to a member of staff.

Pupils surnames will not be used anywhere on the school website or other on-line space in association with photographs or video, unless express permission has been granted by

parents/guardians. Work published on the website will not be identified with an individual pupil. Pupil image file names will not refer to the pupil by name.

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.

Use of cameras and recording equipment by parents/guardians

Parents are welcome to take photographs of their own children taking part in sport and outdoor events. Mobile phones, cameras and other recording devices are not permitted to be used at any time within the EYFS setting. When an event is held indoors, such as a play or concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others.

Photographs and videos taken by parents containing images of other children must not be posted on social network sites or published in any format without the explicit written consent of the parents. Any images taken in school cannot be sold or used for commercial gain without the explicit written permission of the Head.

Data storage and data protection

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

All staff should be aware of the requirement to preserve confidential information held by the school in electronic format concerning staff, parents and/or pupils. Information such as names, contact details and academic information, including reports, should be stored securely and encrypted where appropriate.

Should a data storage device be mislaid or stolen, it is vital that the confidential information cannot be accessed. Staff are advised to hold information which is only absolutely necessary away from the main school server. Staff are required to report immediately any loss of a data storage device which contains pupil details. Staff are also reminded they must not share information or photographs with individuals other than the designated parent and accredited third parties including examination boards.

E-Safety complaints

- Complaints of internet misuse will be recorded on in the Incident Log (Appendix B) and dealt with by the Head.
- Any complaint about staff misuse must be referred to the Head.
- Complaints of a child protection nature must be dealt with in accordance with Child Protection Procedures.
- If a serious breach of the 'E-Safety contract' is discovered, the laptop should be put 'out of order' but not switched off. This is to prevent the contamination of evidence that may be collected by outside agencies (e.g. police) if required.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Last Reviewed: January 2017
Next Review Due: January 2018

E-Safety Policy

Appendix A

Useful resources for teachers

BBC Stay Safe	www.bbc.co.uk/cbbc/help/safesurfing/
Becta	http://schools.becta.org.uk/index.php?section=is
Chat Danger	www.chatdanger.com/
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet	www.childnet-int.org/
Cyber Cafe	http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen	www.digizen.org/
Kent E-Safety Policy and Guidance, Posters etc	www.clusterweb.org.uk/kcn/E-Safety_home.cfm
Kidsmart	www.kidsmart.org.uk/
Kent Police – E-Safety	www.kent.police.uk/Advice/Internet%20Safety/E-Safety%20for%20teacher.html
Leicestershire Constabulary – Internet Watch Foundation	www.leics.police.uk/advice/2_information_zone/50_internet_watch_foundation
Think U Know	www.thinkuknow.co.uk/
Safer Children in the Digital World	www.dfes.gov.uk/byronreview/

Useful resources for parents

BBC	www.bbc.co.uk/schools/parents/cyber_bullying
Care for the family	www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
	www.chatadanger.com
Child Exploitation and Online Protection Centre	www.ceop.gov.uk/
Childnet International "Know It All" CD	http://publications.teachernet.gov.uk
Family Online Safe Institute	www.fosi.org
Internet Watch Foundation	www.iwf.org.uk
Kent leaflet for parents: Children, ICT & E-Safety	www.kented.org.uk/ngfl/ict/safety.htm
Parents Centre	www.parentscentre.gov.uk
Internet Safety Zone	www.internetsafetyzone.com

Appendix B

Chard School

E-Safety Incident Log

Date and time of incident	
Details of incident	
Name of those involved	
Action taken	
Person reporting incident	
Contact details of person reporting incident	

Appendix C

Chard School

ICT Acceptable Use Policy - Pupils

Chard School recognises the importance of ICT in education and the needs of pupils to access the computing facilities available within the School. The school aims to make the ICT facilities it has available for pupils to use for their studies. To allow for this Chard School requires all parents to sign a copy of the Acceptable Usage Policy (AUP). Listed below are the terms of this agreement.

Please read this document carefully and sign and date it in order to indicate your acceptance of the Policy on your child's behalf. It is important that your child understands the policy, so please ensure you take time to explain and discuss it with them.

1. Equipment
    a. Care of the equipment - pupils must look after all equipment provided and treat everything with respect. This includes, making sure that there is no deliberate damage to computer hardware, or change or removal of software.
2. Internet and Email
    a. Content Filtering and use of the Internet - Chard School provides a secure layer of Internet filtering designed to remove controversial, offensive or illegal material that would cause your child to be upset. Chard School ensures that
        i. All access to the Internet is supervised by adults
        ii. Children are not allowed access to chat rooms at any time
        iii. Children are taught about safe Internet use by their teachers.
    b. Email - As part of your child's work in ICT and other subjects, we offer supervised access to the Internet. On some occasions children may be offered the opportunity to use email outside the school, for example to communicate with children from other schools.
3. Mobile technologies
    For reasons of safety and security your child is not permitted to bring a mobile phone or other technology to school. They should not use their mobile or any other technology outside of school in a way that is likely to damage the reputation of the school or risk the welfare of other pupils or adults that work within the school. If inappropriate material is sent to a pupil, it must be reported immediately to a member of staff within the school.

I have read the Pupil Acceptable Use Policy and I have discussed it with my child. I agree for my child

Name of child …….…… Class …….

to use the Internet and email in accordance with the school guidelines.

Signature…….…… Date…….

Full Name…….…… (printed)

Please return to the School office in first week of term

Appendix D

Chard School

ICT Acceptable Use Policy – Staff, Governor, Visitor

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I will only use the school's email/internet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system for any business.
- I will ensure that personal details are kept secure and are used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Head.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Head.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on the request of the Head.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- If I am in the EYFS setting, my personal devices will be put away and not used in the setting.
- I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the Safe Use of ICT throughout the school.

Signature…….…… Date…….

Full Name…….…… (printed) Job Title …….

Return to School office for personnel file

Appendix E

Notes on the legal framework of e-safety

Sexual Offences Act 2003

- Grooming: If you are over the age of 18 years and have communicated with a child under the age of 16 years at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
- Making indecent images: It is an offence to take, make, distribute, show or advertise indecent images of a child under the age of 18 (NB – to view an indecent image on your computer means that you have made a digital image).
- Causing a child under the age of 16 to watch a sexual act: It is an offence to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
- Abuse of a position of trust: Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under the age of 18 years, with whom they are in a position of trust (this applies to teachers, social workers, health professional and connexions staff).

Communications Act 2003

There are two separate offences under this act

- Sending by means of public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
- Sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

The Computer Misuse Act 1990

It is a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data.

Public Order Act 1986

It is an offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Malicious Communications Act 1988

It is an offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information, with the intent to cause distress or anxiety to the recipient.

Copyright, Designs and Patents Act 1988

It is an offence to use unlicensed software.

Protection from Harassment Act 1997 (Section 2)

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.