CARFAX COLLEGE

E-Safety Policy

2015 (updated 2018)

Contents

1. Rationale of the policy

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Carfax College (CTE) with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of CTE.
- assist College staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The main areas of risk associated with the use of ICT-based technologies by young people can be summarized as follows:

	Commercial	**Aggressive**	**Sexual**	**Values**
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	extremist ideology/ terrorism other unwelcome bias/prejudice (e.g. racism) misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting / yipsy	providing misleading info and advice health and wellbeing; time spent online

(adapted from material by Ofsted, 2014)

Acronyms and jargon are common place in technology and often obscure meaning and understanding. The following link provides access to a wide ranging glossary of technological terms in current use: http://www.digizen.org/glossary/.

2. Scope of the policy

This policy applies to anyone who uses ICT-based technologies within the school or who has access to the school's ICT systems, whether on school premises or not.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside the school but nevertheless be linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

3. Roles and responsibilities

ROLE	KEY RESPONSIBILITIES
Representives of the Proprietor	• To approve the e-safety policy • To review the effectiveness of the policy.
Principal	• To take overall responsibility for e-safety provision • To ensure that there are appropriate filters in place on any access to the Internet via the school's ICT systems • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Designated Child Protection Lead

ROLE	KEY RESPONSIBILITIES

Designated Safeguarding Lead	• To take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
	• To promote an awareness and commitment to e-safeguarding throughout the school community
	• To liaise with school ICT technical staff
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• To facilitate training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• To remain regularly updated on e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Tutors	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
Management and administrative staff.	• To read, understand and help promote the school's e-safety policies and guidance • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use • To report any suspected misuse or problem to the Designated Child Protection Lead • To maintain an awareness of current e-safety issues and guidance • To model safe, responsible, and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school approved systems, never through personal mechanisms, e.g. email, text, mobile phones, social media, etc., in accordance with the College Staff Code of Conduct.

ROLE	KEY RESPONSIBILITIES
Pupils	• To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies outside school and realise that the school's E-Safety Policy covers their actions outside school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
Parents	• Promote good online safety practices • to consult with the school if they have any concerns about their children's use of technology
Host Families	• To read, understand and help promote the school's e-safety policies and guidance • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use • To report any suspected misuse or problem to the Designated Child Protection Lead • To maintain an awareness of current e-safety issues and guidance • To model safe, responsible, and professional behaviours in their own use of technology

4. Pupil Education
The education of pupils in online safety / digital literacy is an essential part of the College's online safety provision.

- Online safety sessions are delivered once per term as part of the PHSE curriculum.
- Key online safety messages are reinforced as part of pastoral activities and personal tutor sessions
- New pupil enrolment comprises a discussion of e-safety and summary of College rules
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

5. Staff and Host Family Education

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training is made available to staff via *Boost*.

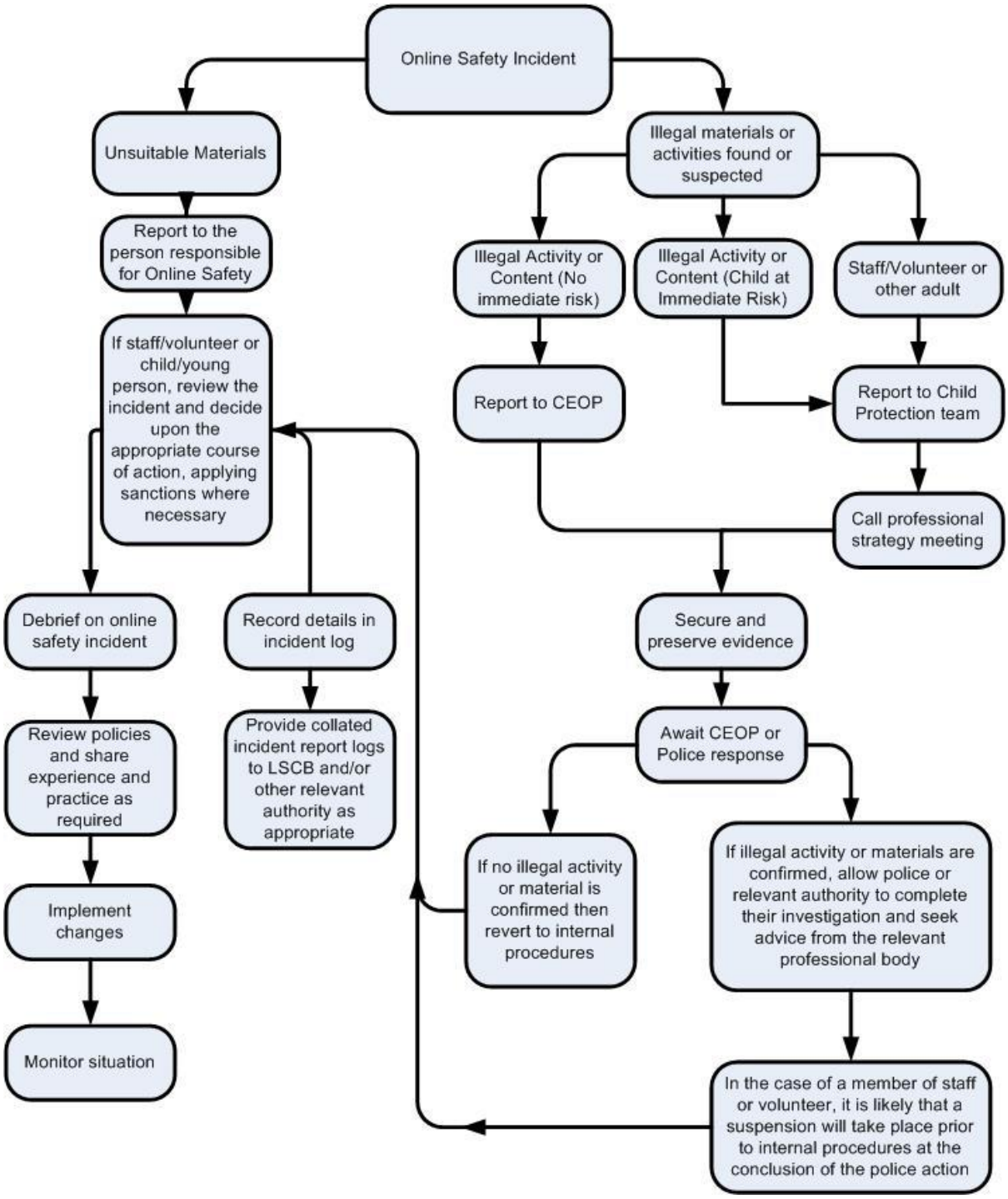
- All new staff and host families receive online safety training as part of their induction programme, ensuring that they fully understand the College e-Safety Policy and what to do should an incident arise.

- Host Families receive an annual briefing from the Dame on e-safety, along with other safeguarding issues. The Dame also sends out regular emails reminding host families of e-safety issues.

6. Responding to incidents of misuse

It is hoped that all members of the College will be responsible users of digital technologies, who understand and follow College policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Responses to infringement depend on the content and have been categorised as "illegal and unacceptable" and "unacceptable." Please refer to Table 1 for examples of each category.

5.1 Responding to "unacceptable and illegal material"
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to the Oxfordshire Thames Valley police on 01865 841 148.



5.2 Responding to "unacceptable material"

In the event that it is suspected unacceptable material is being used, ensure the following procedure is followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- If the misuse is on the College premises then it should be reported immediately to the Principal, DSL or Deputy DSL.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

- Ensure relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and stored in the file for investigation (except in the case of images of child sexual abuse – see below)

Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

o Internal response or discipline procedures

o Involvement by Oxfordshire Safeguarding Children's Board

o Police involvement and/or action

It is important that all of the above steps are taken as they will provide an evidence trail for the College and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. A file of notes should be retained for evidence and reference purposes.

5.3 Incidents of misuse in "out of hours" contexts

If the misuse is discovered by a host family out of hours then the host family must evaluate the seriousness of the suspected activity (refer to Appendix 1).

If the misuse puts a child at risk then they must call the LADO immediately in accordance with the College safeguarding policy. If the misuse is illegal then they must call the police immediately.

If the misuse is unacceptable then they must report it to the Dame on the emergency number out of hours.

All other e-safety concerns should be reported to the Dame within one working day of the concern having been raised.

6. Sanctions

- Possible sanctions for infringements by pupils or staff include:
    - interview/counselling by Designated Child Protection Lead / Principal;
    - informing parents / carers;
    - removal of Internet or computer access for a period;
    - referral to LA / Police.

- Complaints of cyberbullying are dealt with in accordance with the school's Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

7. Further Information

Websites

UK Council for Child Internet Safety (UKCCIS):
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Child Exploitation and Online Protection Centre (CEOP): http://ceop.police.uk/

UK Safer Internet Centre: http://www.saferinternet.org.uk/

Childnet International: http://www.childnet.com/

Parentzone: http://www.theparentzone.co.uk/

Publications

The safe use of new technologies (090231), Ofsted, 2010
www.ofsted.gov.uk/resources/090231

Safer children in a digital world: the report of the Byron Review, DCSF and DCMS, 2008
http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews

Ofcom's response to the Byron Review, Ofcom, 2008
http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/

Appendix 1

Examples of misuse categories
Illegal and unacceptable misuse
Child Sexual abuse images.
Grooming, incitement, arrangement or facilitation of sexual acts against children.
Possession of an extreme pornographic image
Material intended to stir up hate related activity
Unacceptable misuse
Pornography
Promotion of any kind of discrimination
Threatening behaviour
Promotion of extremism or terrorism
Other offensive material
Using systems that bypass College filters
Infringing copyrights
Revealing confidential material
Creating or propagating computer viruses