Online Safety Policy

November 2016

Approved by GB: Nov 2016

Next review due: Nov 2019

Online Safety at Churchfields Junior School

Introduction

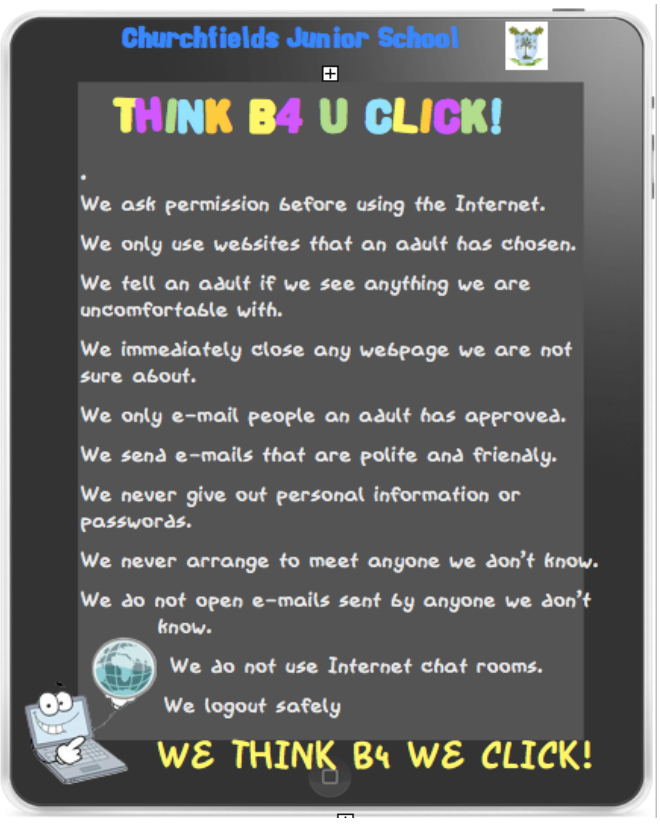
Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever-earlier age. All users need to be aware of risks associated with the use of these Internet technologies. At Churchfields Junior School we understand the responsibility to educate our pupils in Online Safety issues; teaching them the appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for Online Safety has been designated to the Online Safety Officer (Andrew Wilkins), Computing Leader (Andrew Wilkins) and Child Protection Officer (Wendy Thomas and Rebecca Emeny). All members of the school community have been made aware of who holds the above posts. It is the role of the Online Safety Officer to keep abreast of current issues and guidance through organisations such London Borough of Redbridge, CEOP (Child Exploitation and Online Protection) and Childnet.

Introducing the Online Safety policy to pupils

- The Online Safety rules "Think B4 U Click" will be displayed in all classrooms and the Computing suite and discussed with the pupils at the start of each year. Online Safety content will be embedded throughout the Computing curriculum, and introduced when necessary and relevant pupil activities require it. Online Safety will also be taught at relevant points throughout the school curriculum for example, during PSHE lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored**.**
- Pupils in Years 5 and 6 will also receive a discrete Online Safety lesson in the middle of the Autumn Term, to be taught by the Computer Leader. This will cover mobile phone usage and usage of apps such as Whatsapp and Instagram and aspects of the Prevent agenda.



- An Online Safety assembly will be presented to pupils each year and again during "Safer Internet Day" in February.

- During Online Safety week pupils are invited to take part in an Online Safety competition to encourage safe practice online. This will be organised by the Digital Leaders, and directed and led by the Computing Leader.

Responsibilities of all staff

- To provide a safe environment in which children can learn.
- Report any concerns on a child's use of technology, both within the school environment and outside, to the school safeguarding lead.
- Sign and review and sign the school's Acceptable Use Agreement
- Engage with and attend Online Safety training delivered by the Computing Leader.
- To use school equipment for the educational purposes for which it was intended. This means not storing personal images, emails, etc. on school computers, camera and tablets.
- Report any concerns around breeches in network filtering, cyber security and inappropriate usage of school equipment and resources.

Online Safety skills development for staff

- Our staff receive regular information and training on Online Safety issues through the Computing Leader at staff meetings.
- All teaching and non-teaching staff will take part in an annual Online Safety INSET.
- All teaching and non-teaching staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of Online Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff receive information on the school's Acceptable Use Agreement (see appendix 1) as part of their induction.
- All teaching and non-teaching staff are encouraged to incorporate Online Safety activities and awareness at the start and within each Computing lesson.
- All teaching and non-teaching staff will have access to the Online Safety Policy and this will be shared annually.
- All staff will be informed of the need to restrict internet access at school to professional usage only, and that personal usage is discouraged.

Online Safety information for parents/carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website or on the Fronter Learning Platform.
- The school website contains links to sites like Thinkuknow, Childline, CEOP and the CBBC Web Stay Safe page.
- The school website contains useful child-friendly information on the Online Safetyrules, "Think B4 U Click".
- The school will send out relevant Online Safety information through newsletters, the school website, email and text message, and the school prospectus.
- Parents/carers are invited to attend an annual Online Safety workshop to look at the benefits and risks of online behaviour.

Sexual and Online Abuse

- Staff should be aware that sexual abuse can occur via the internet and can involve a range of activities, including but not limited to online grooming and exploitation, exposure to pornographic content and engaging a child in sexual activity online.

- Staff and pupils should be aware that perpetrators can be male or female and may include children themselves (such as in cases of sexting).
- Pupils in Year 5 and 6 will receive a discreet Online Safety lesson explaining how they can avoid online abuse and the importance of reporting it to an adult.
- 'Sexting' can be defined as 'an increasingly common activity among children and young people, where they share inappropriate or explicit images online…' This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.
- Staff should be aware that they themselves can be the victim of online abuse. If they feel they are being abused online, staff should report the incident to SLT.

Radicalisation

- Staff receive 'Prevent' training to identify signs of radicalisation amongst their pupils.
- Staff should be aware that the internet could be a tool in the radicalisation of young people and also in the potential accidental and deliberate exposure of young people and adults to extremist views and content.
- Staff should report any concerns on a child's use of technology, both within the school environment and outside, to the school safeguarding lead.

Teaching and Learning

Internet use will enhance learning

- The school will provide opportunities within a range of curriculum areas to teach Online Safety.
- The computing scheme of work, "Switched on ICT" integrates Online Safety within each lesson and is progressive in each year group.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access will be designed expressly for pupil use and will include active filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- Pupils will be encouraged to "turn off the monitor and inform an adult" to hide any material that they know is unsuitable for viewing. This will instantly cover the whole screen until it can be dealt with by the class teacher.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- All staff using the Internet with pupils will screen websites and videos prior to lessons to ensure both are appropriate for viewing and to avoid inappropriate pop-ups.

Managing Internet Access

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Advice on security strategies will be monitored on the School's webpage and clarification sought as necessary.

E-mail

- Pupils may only use approved e-mail accounts (currently via the MLE Fronter) on the school system and email usage should be supervised and monitored by a staff member.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Parents should only email the school office email, and the office will forward messages to the relevant staff. Staff should not email parents directly, but via the main school office.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff should report spam emails and compromised email accounts immediately to the technical support company (Joskos) and the Computing Leader.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the school website should be the school address, e-mail 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.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified with their full name.
- Pupils' full names will not be used anywhere on the website.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents as agreed by parents on the Acceptable Use Agreement (AUA).

Social networking and personal publishing

It should be remembered that networks such as Twitter, Facebook and TES Connect can offer teachers connections with a range of global educators. Such networks can also help maintain work life balance as they allow communication with family and friends. However the use of social network sites is strictly forbidden in school, except when officially representing the school. If you use them outside school, it is best that you do not refer to anyone in our school community, especially the pupils. If you do refer to adults, then please ensure it is always in a positive light. It is your responsibility to ensure that you protect both the reputation of the school and your own professional reputation. Beware that referring to colleagues, pupils or parents in a negative light could be deemed as defamation and amount to legal proceedings. Staff should not accept friend request or maintain online social relationships with pupils or parents. All contact with parents needs to be via school safe email.

Images of pupils should not be posted, tagged or published. The place for such images is via the school website or Fronter pages.

- The school will restrict access to social networking sites.
- The operation and maintenance of the school's presence on social networking services will be monitored by the Computing Leader.
- Content uploaded to future school accounts with Instagram and Twitter will be monitored and comments will be deactivated.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- All school staff should be aware that abuse, neglect and safeguarding issues are rarely standalone events that can be covered by one definition or label. In most cases multiple issues will overlap with one another.
- Parents will have the opportunity to attend an Online Safety talk where they will learn about how to safely monitor their child's use of social networking.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- Staff shall not access or use social networking sites through the school network.
- Staff will be supported when ensuring their presence on social network is set to private and privacy settings are enabled.

Managing filtering

- The school will work with the London Borough of Redbridge and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to either the Online Safety Officer or Child Protection Officer.
- Staff should conduct Internet searches outside of class time, and without the presence of pupils to ensure accidental inappropriate results are not viewed by pupils.
- The Online Safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting personal data

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

Policy Decisions

Authorising Internet access

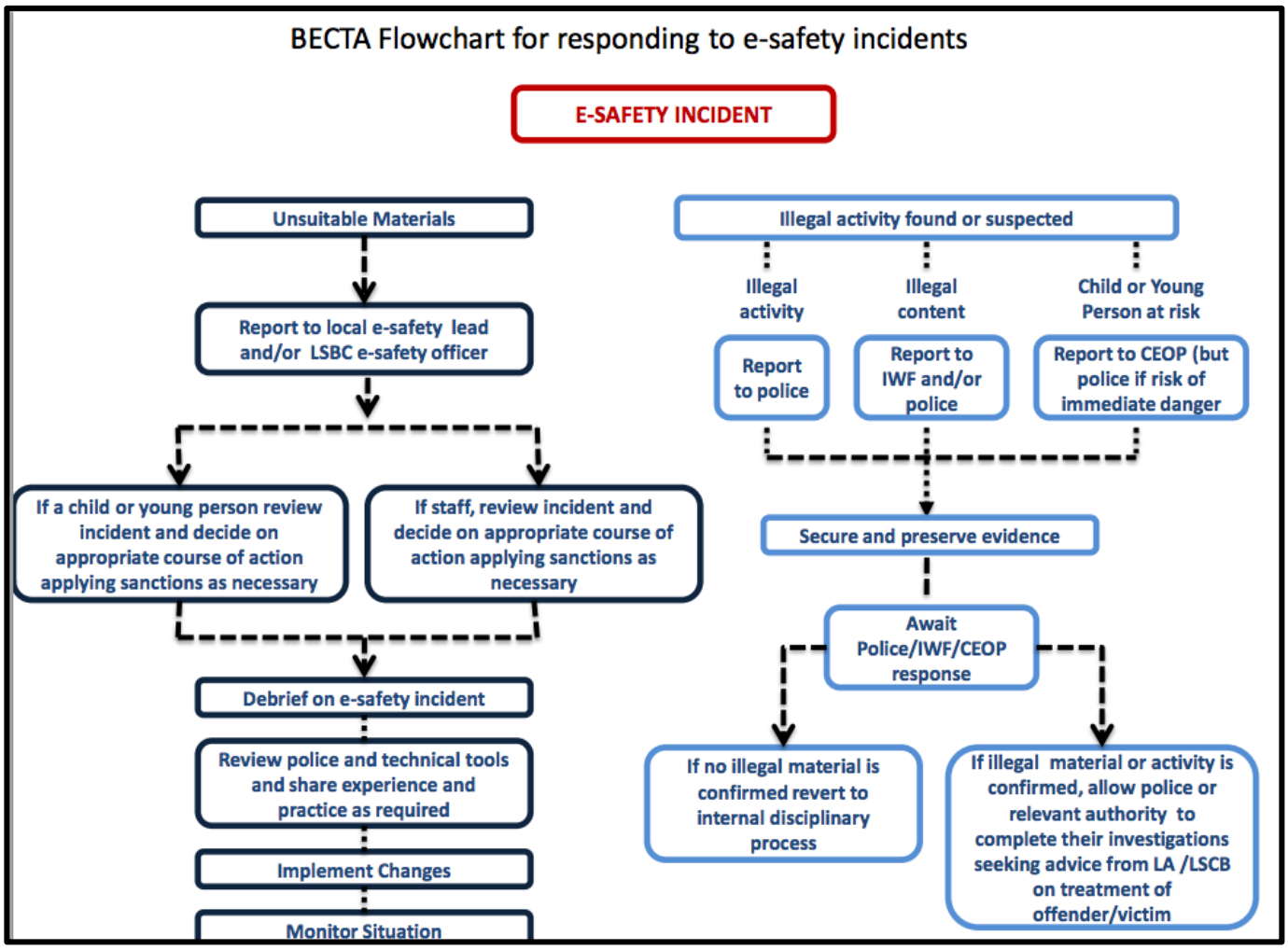
- Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Acceptable Use Agreement for pupils and abide by the school's Online Safety rules "Think B4 U Click". These Online Safety rules will also be displayed clearly in all networked rooms.
- Access to the Internet will be by directly supervised access to specific, approved on-line materials.
- Pupils will only be permitted to use school computer equipment when in the presence of a member of staff. No pupils shall be permitted to be in the computing suite unsupervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's Online Safety rules and within the constraints detailed in the school's Online Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school computing resource.

Password Security

- Adult users are provided with an individual network, email and Fronter Learning Platform login username and password, which they are encouraged to change periodically.
- All pupils are provided with an individual network, email and Fronter Learning Platform login username and password.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others within the school community.
- All staff should log off their computers when leaving their terminal unattended.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

Reporting

- Where internet misuse has occurred all staff follow the appropriate channels (see Appendix 2 below)
- Internet misuse will be dealt with by a senior leader, the Child Protection Officer and/or Online Safety Officer.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Reports of a child protection nature must be dealt with in accordance with school Safeguarding procedures.
- Pupils and parents will be informed of the reporting procedure.



Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor London Borough of Redbridge can accept liability for the material accessed, or any consequences of Internet access.

The school will audit computing provision to establish if the Online Safety policy is adequate and that its implementation is effective.

The Learning Platform

- All staff will be trained and given advice on how to effectively use the Fronter Learning Platform.
- Parents will be informed about what the Fronter Learning Platform is and how it can enhance the learning of each child.
- All children will be given training on how to effectively use the Fronter Learning Platform.
- All children will be given a username and password to access secure resources and facilities through the Fronter Learning Platform. Pupils taught to keep their password secure.
- The Fronter Learning Platform will be regularly monitored for incidents of cyber-bullying, inappropriate use of language or the uploading of inappropriate files. Children will be informed that the sending of messages through the Fronter Learning Platform is monitored and misuse of the messaging system will result firstly in a warning, then a notification to

parents and possible removal of the messaging service of the Fronter Learning Platform should such behaviour be repeated.

- Children will be allowed to upload photographs of groups or group activities onto their homepage but not individual pictures of themselves.
- Class teachers will monitor the use of the Fronter Learning Platform. Any misuse of the Fronter Learning Platform will be reported to the Head Teacher.

Review

This policy is implemented on a day-to-day basis by all staff. It is monitored by the Online Safety Officer and Computing Leader.

On-going incidents will be reported to the Governing Body.

This policy is reviewed by staff, Online Safety Officer and Computing Leader at least once every three years, and reviewed whenever Government policy changes. Parents are most welcome to see copies of this document on the schools' website and comments are invited from anyone involved in the life of the school.

Appendix 1

Acceptable Use Policy (AUP): Staff Agreement Form

Covers use of digital technologies in school: i.e. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity (on social networking sites) that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. This is currently Staff Mail.
- I will only use the approved school email, school MLE (Managed Learning Environment) or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff and will not store images at home without permission.
- I will use the school's Learning Platform in accordance with school / and London Grid for Learning advice.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role, and that these are secured and private.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's Online Safety curriculum into my teaching.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

Acceptable Use Policy (AUP): Staff agreement form

User Signature

I agree to abide by all the points above.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

Authorised Signature (Head Teacher)

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)

Useful Links and Resources

Glossary of technology-related terms

https://www.salford.gov.uk/media/380874/glossary-of-terms-used-on-the-internet.pdf

NSPCC Online Safety advice

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

NSPCC Sexting

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

Childline Radicalisation

https://www.childline.org.uk/info-advice/your-feelings/anxiety-stress-panic/worries-about-the-world/?gclid=CLfrq6H6idACFcQV0wod7mcOtg