BURE PARK PRIMARY SCHOOL

Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY) POLICY

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

The school has a duty to provide pupils with access to quality learning using internet technologies and, with this, the responsibility to ensure that this learning takes place safely. We aim to educate children about the benefits and risk of using new technology and social media, and equip them with the skills to manage themselves safely, while using technology inside and outside of school. Additional guidance and resources for parents and carers can be found on the 'E-Safety' page on the school website, as well as updates on the app.

This policy recognises our commitment to keeping children safe and acknowledges its part in the school's overall Safeguarding policies and procedures.

Essential Skills

We aim to ensure:

- Responsible ICT and social media use by all staff and pupils.
- Sound implementation of the overarching safeguarding policies in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Oxfordshire Local Authority including the effective management of content filtering.

SCHOOL Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY) POLICY:

Managing Internet Access:

- All staff, volunteers and students must read and sign the 'Staff Acceptable Use of Technology & Social Media Agreement' and any new staff before using any school ICT resource. These agreements will be kept in the 'safeguarding folders'.
- Children and parents are required to sign a 'Pupil Parent School Agreement', derived from the SMART rules.
- E-safety is to be taught and referred to regularly, in accordance with the e-safety curriculum. Children should follow the SMART rules in school to remain safe.
- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to ICT Management Company to block the site.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.

- The School's filters will block sites which are deemed to contain inappropriate material or content.
- Pupils may only use approved e-mail accounts in school, as part of curriculum teaching.

Staff Guidance on the use of Social Networking and Professional Conduct Online:

Please refer to 'E-conduct guidance for staff' and follow the additional guidance below:

- It is never acceptable to accept a friendship request from a child from the school as in almost all cases children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.
- Staff who wish to engage with social media sites, such Facebook, Twitter or Instagram etc, should be aware that they are representatives of the school and they should not engage with or post comments which affect the professional identify of the school or can be considered inappropriate in nature or defamatory in nature, be it libellous or slanderous.
- Staff are required to follow theses guidelines and demonstrate acceptable conduct at all times when using the school's IT systems and also act in a professional manner when accessing the internet from home. The school and Local Authority will be informed in the case of misuse or unprofessional conduct.
- Staff may only take photos in school, for school use, on school provided ipads or technology and not on personal devices.
- Any images of children within the school that are posted on the website or blog, will have the required parental permission in line with current GDPR requirements.

Managing Emerging Technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out, if required, before use in school is allowed.
- Mobile phones are not allowed to be used by pupils in school and staff are aware that they will not be used for personal use during lessons or formal school time, unless during emergencies. The sending of abusive or inappropriate text messages, files by Bluetooth or any other means is forbidden.
- Staff should use a school phone where contact with parents is required.
- Any device which may capture or record an image, or connect to the internet, belonging to a pupil, must be left with the class teacher.

Information System Security:

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

Assessing Risks:

- 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. Neither the school nor OCC can accept liability for the material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the policy is adequate, effective or in need of modification and that the implementation of the 'Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY)' policy is appropriate.

Handling e-safety Complaints:

- Complaints of Internet misuse will be dealt with by the SLT.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures and policy.
- Any instance will be managed appropriately with due regard to confidentiality.
- For procedure see Appendix A.

Use of ICT Equipment :

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite. The school provides portable ICT equipment such as ipads, laptop computers, voice recorders, video cameras and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

- The school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited.
- If an individual leaves the employment of the school, any equipment, e.g. laptops, ipads, cameras etc must be returned, and email accounts will be deactivated.

Communication of Policy:

Pupils:

- Pupils will follow the SMART rules, which are displayed across school.
- Pupils will be informed that Internet use will be monitored.
- An E-Safety Home-School agreement is sent home annually, to be discussed between parent or guardians and children, and returned to school signed.

Staff:

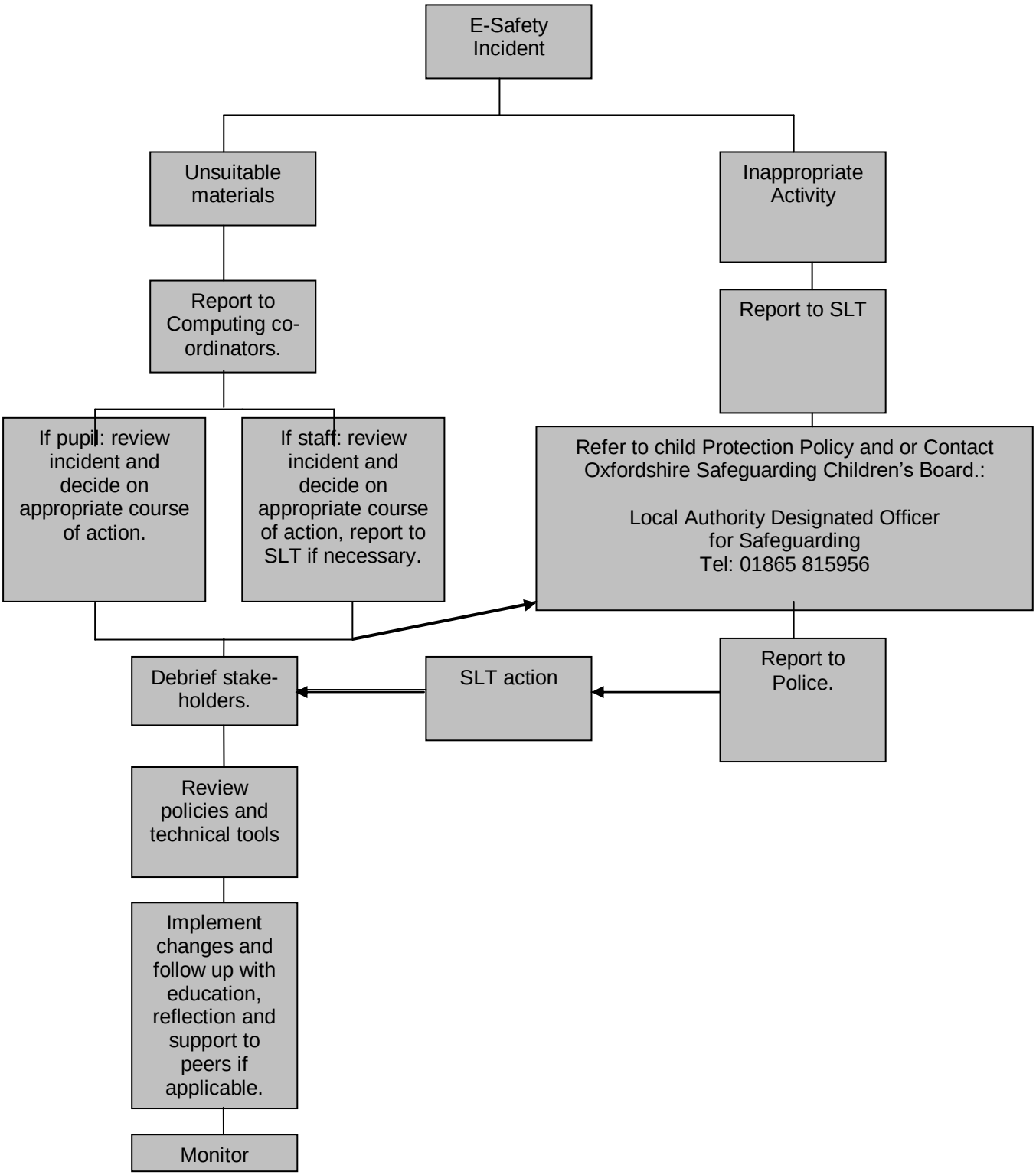
- All staff will be given access to the School Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY) and its importance explained.
- Staff should be aware that the LA monitor Internet traffic and can trace it to the individual user. Discretion and professional conduct is essential.
- All staff to read, agree, sign and remain aware of the school 'Staff Acceptable Use of Technology & Social Media Agreement'.

Parents:

- Parents' attention will be drawn to the School Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY) policy on the school Web site.
- The school will ask all parents and pupils to sign a Pupil/Parent/School e-safety agreement.

Appendix A

Flowchart for responding to e-safety incidents in school



Appendix B

Useful resources for teachers

Think U Know
www.thinkuknow.co.uk

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing

Chat Danger
www.chatdanger.com

Child Exploitation and Online Protection Centre
www.ceop.gov.uk

Childnet
www.childnet-int.org

Digizen
www.digizen.org

Kidsmart
www.kidsmart.org.uk

Useful resources for parents
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

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone
www.internetsafetyzone.com

This list is not exhaustive and more resources can be found on the school website.

Appendix C
E-Safety Audit – Primary Schools

This quick self-audit will help the senior leadership team (SLT) assess whether the e-safety basics are in place in conjunction with the safeguarding and child protection policies and audits.

Has the school a Safeguarding Children and Young People in the Context of Technology and Social Media (E-SAFETY)Policy that complies with OFSTED guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff:	
And for parents on the website:	
The designated Child Protection Lead is Yvonne Hewson and the Deputies are: Karen Ward, Pam Cotter and Rachael Howells.	
Has e-safety training been provided for both pupils and staff?	Y/N
Do staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Y/N
Are the SMART Rules displayed in all rooms with computers?	Y/N
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N