Blenheim

Management of Online Safety Policy

Committee: Community

Date Published: May 2019

Expiry Date: May 2021

www.blenheim.surrey.sch.uk

Tel: 01372 745333 Email: headteacher@blenheim.surrey.sch.uk
follow us on Twitter @BlenheimEpsom

It is a school priority to provide facilities, new technologies and a learning environment to enable all students to achieve their potential now and in the future. The introduction of new technologies provides exciting opportunities to develop teaching and learning but also presents a range of challenges. The purpose of this policy is to ensure that the school has in place robust procedures and mechanisms to safeguard the welfare and security of both students and staff whilst enabling it to maximise the benefits new technologies bring to the education of students at the school.

This policy should be read in conjunction with the Child Protection and Safeguarding Policy.

In order to maintain the safety and security of both students and staff the school will maintain the security of all information systems; robustly risk assess access to the internet and have in place controls and protocols for managing such access; develop comprehensive communications and training programmes for both staff and students and, where appropriate, for parents/carers; and ensure full consultation with parents/carers prior to the introduction or development of any new technology.

- Staff will be required to sign an ICT Acceptable Use Agreement to underpin their professional use of ICT which is consistent with the school ethos and policies, and the law.

- Students will be required to sign an ICT Acceptable Use Agreement on entry to the school, and thereafter annually.

- Students joining the iPads for Learning scheme are required to sign an iPads for Learning scheme Agreement form in addition.

- At regular intervals Governors will review the impact of new technologies on teaching and learning within the school, including issues of safeguarding and security.

1. Teaching and Learning

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger.

Online Safety covers issues relating to children and young people as well as adults and their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on

risks and responsibilities and is part of the 'duty of care' that applies to everyone working with children.

1.1 Why Internet and digital communications are important

- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Students will be shown how to research, publish and present information appropriately to a wider audience.

1.2 How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased student attainment and motivation.

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between students worldwide;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- access to learning wherever and whenever convenient, encouraging independent learning.

1.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The school will ensure that information regarding copyright law is made available to staff and students, eg by displaying advisory posters in suitable locations to ensure the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law.
- Access levels to the Internet will be reviewed annually to reflect the curriculum requirements and the age and ability of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and ability.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

1.4 How will students learn how to evaluate Internet content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular, it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach is required.

Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for students to develop skills in evaluating Internet content. For example, researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of.

- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Students will use appropriate tools to research Internet content, eg Google or Safari for text-based resources, Wolfram Alpha for research in STEM subjects and Safari Image Search for photos and images.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum, as well as being addressed in core IT lessons.

2. Managing Information Systems

2.1 How will information systems security be maintained?

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. For students and staff, flouting the acceptable use policy could be regarded as a disciplinary matter.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.
- On and offsite storage of backup media must be secure as sensitive data is held.

Wide Area Network (WAN) security issues include:

- Broadband firewalls are configured to prevent unauthorised access to school systems
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.

- Files held on the school's network will be regularly checked for viruses, Trojans etc.
- The Network Manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

In the school context (as in the business world), email should not be considered private and the school reserves the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of students and staff and the preservation of human rights, both of which are covered by recent legislation. It is important that staff understand they should be using a work provided email account to communicate with parents/carers, students and other professionals for any official school business. This is important for confidentiality and security and also to safeguard members of staff from allegations. Personal emails should not be provided.

2.2 How will email be managed?

- Students may only use their school email accounts for school purposes.
- Students must immediately tell their class or Form Tutor if they receive offensive email. The Online Safety Administrator (Linda Baker) should then be informed if appropriate.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts to communicate with students and parents/carers.
- Email sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper would be. If in any doubt about the appropriateness of an email, staff should ask their Line Manager for guidance.
- Staff should not use personal email accounts for professional purposes.

2.3 How will published content be managed?

- Images or videos that include students will be selected carefully.
- Students' full names will not be used anywhere in electronic publications, when associated with photographs.
- Written permission from parents or carers will be obtained before images/videos of students are electronically published.

2.4 How will social networking, social media and personal publishing be managed?

Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

All staff will be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger.

- IT Services will control access to social media and social networking sites.
- Students will be advised never to give out personal details of any kind that may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging (IM) and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Leadership Team before using Social Media tools in the classroom. This is not necessary for the following sites: Edmodo and Showbie.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis.
- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the Staff ICT Acceptable Use Agreement.

2.5 How will filtering be managed?

Levels of Internet access and supervision will vary according to the student's age and experience. Access profiles must be appropriate for all members of the school community. Older students, as part of a supervised project, might need to access specific adult materials; for instance, a course text or set novel might include references to sexuality. Teachers might require students to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

Occasionally mistakes may happen, and inappropriate content may be accessed. It is therefore important that students should always be under supervision, ie by the class teacher when using the Internet and that the Acceptable Use Policy is enforced. In addition, Internet Safety Rules should be displayed, and both students and adults should be educated about the risks online. There should also be an Incident Log in PARS to report breaches of filtering or inappropriate content being accessed.

Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF), Surrey Police or Child Exploitation and Online Protection Centre (CEOP).

Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the students. Often this will mean checking the websites, search results etc just before the lesson. A site considered safe one day may be changed due to the Internet being a dynamic entity. Particular attention should also be paid to advertisements as they can change each time the web page is accessed.

- The school's broadband access will include filtering appropriate to the age and maturity of students.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) should be made aware of this procedure.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

2.6 How should personal data be protected?

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

3. Policy Decisions

3.1 How will Internet access be authorised?

- The school will maintain a current record of all students who are granted access to the school's electronic communications.
- All staff will read and sign the Staff ICT Acceptable Use Agreement (AUA) before using any school ICT resources.
- Parents new to the school will be asked to read and sign the School Acceptable Use Agreement for student access and discuss it with their child, where appropriate.
- Students will be presented with the AUA onscreen, half termly, as a reminder.

3.2 How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Surrey Police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

3.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Online Safety Administrator will record all reported incidents and actions taken in the School Online Safety incident log and refer to others regarding other relevant areas e.g. Bullying or Child Protection log.
- The DSL, DDSL or DSO will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage online safety incidents in accordance with the school discipline/ behaviour policy where appropriate.
- The school will inform parents/carers of any incidents or concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or Online Safety officer and escalate the concern to the Police. See Appendix 1.

3.4 How will Online Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- All Online Safety complaints and incidents will be recorded by the school, including any actions taken.

3.5 How will Cyberbullying be managed?

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual bullying, which can occur in or outside school. Cyberbullying can be defined as "A different form of bullying and can happen at all times of the day, with a potentially bigger audience and more accessories as people forward on content at a click". (DfE Preventing and tackling bullying July 2017)

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parents/carers of students will be informed.
    - The Police will be contacted if a criminal offence is suspected.

3.6 How will mobile phones and personal devices such as iPads be managed?

- The use of mobile phones and other devices such as iPads by students and staff in school will be decided by the school and covered in the school Acceptable Use or Mobile Phone Policies.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices such as iPads is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or iPad if they believe it is being used to contravene the school's behaviour or bullying policy. The phone or iPad can be searched by the Leadership team without the consent of the student or parent/carer (DfE Searching, Screening and confiscation. Jan 2018). The reason for searching the phone/iPad must be consistent with the reason for confiscation. The Headteacher or staff authorised by him have statutory powers to search students or their possessions, without their consent where there are reasonable grounds for suspecting they have a 'prohibited item' eg a pornographic image or any item reasonably suspected may be used to commit an offence. Data or files on any electronic device may be examined if there is a good reason to do so. Any data or files may be erased if there is a good reason to do so. In determining a 'good reason' to examine or erase data and files, the staff member must reasonably suspect that the data or file on the device has been, or could be used to cause harm, to disrupt teaching or break the school rules. If there is suspicion that the material on the device may provide evidence relating to a criminal offence the device will be handed over to the police for further investigation.
- Mobile phones (KS5) and iPads (KS3/4/5) may be used during lessons or formal school time if part of an approved and directed curriculum-based activity with consent from a member of staff.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.

Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- Mobile phones and iPads are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

Students Use of Personal Devices
- If a student breaches the school policy then the phone or iPad will be confiscated and will be held in a secure place normally for the remainder of the day.
- Phones and iPads must not be taken into examinations. Students found in possession of either during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his/her parents/carers s/he will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone or iPad during the school day, but to contact the school office.

Staff Use of Personal Devices
- Staff are not permitted to use their own personal phones or devices for contacting students and their families within or outside of the setting of their professional capacity.
- Staff will be issued with a school phone where contact with students or parents/carers is required.
- Where possible, staff will only use work-provided equipment to take photos or videos of students. Where personal devices such as mobile phones or cameras are used, the images should be downloaded onto the school system and deleted from the personal device so images are not removed from site.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Sanctions for misuse of Blenheim ICT facilities

Note: depending on the severity of the infringement, these stages may be bypassed to the appropriate level. Incidents involving cyberbullying, racism or homophobia will be dealt with reference to the appropriate policy.

First Offence

- The student will receive a warning, with the particular infringement of the AUA discussed with a member of staff.
- The incident and response will be logged in PARS

Second Offence

- A letter or email will be sent to parents/carers, informing them of the incident
- The student will have restrictions placed on their use of the ICT facilities. The student may receive further sanctions depending on the nature of the offence
- The Head of Year will be informed
- The incident and response will be logged in PARS

Third Offence

- A further letter or email will be sent to parents/carers informing them of the incident
- The student will have restrictions placed on their use of the ICT facilities. The student may receive further sanctions depending on the nature of the offence
- The Head of Year will be informed
- The incident and response will be logged in PARS

4. Communication Policy

4.1 How will the policy be introduced to students?

- All users will be informed that network and Internet use will be monitored.
- An Online Safety training programme will be established across the school to raise the awareness and importance of safe and responsible Internet use amongst students.
- An Online Safety module will be included in the ICT programmes covering both safe school and home use.
- Online Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Online safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

4.2 How will the policy be discussed with staff?

- The Online Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or their actions have undermined confidence in their professional abilities.

4.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school Online Safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting online safety at other attended events e.g. parents' evenings.

- Parents are given weekly updates through the Heads bulletins, with current information on various ways of how to support students to keep safe online.
- Parents will be encouraged to read the school Acceptable Use Policy for students and discuss its implications with their children.
- Parents and students will be requested to sign the AUA as part of the Home School Agreement.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parent

Online Safety Contacts and References

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

Childline: www.childline.org.uk

Childnet: www.childnet.com

Uk Safer Internet: https://www.saferinternet.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kent e–Safety in Schools Guidance:
http://www.kelsi.org.uk/pupil_support_and_wellbeing/safety,_health_and_wellbeing/child_protection_safeguarding/e-safety.aspx

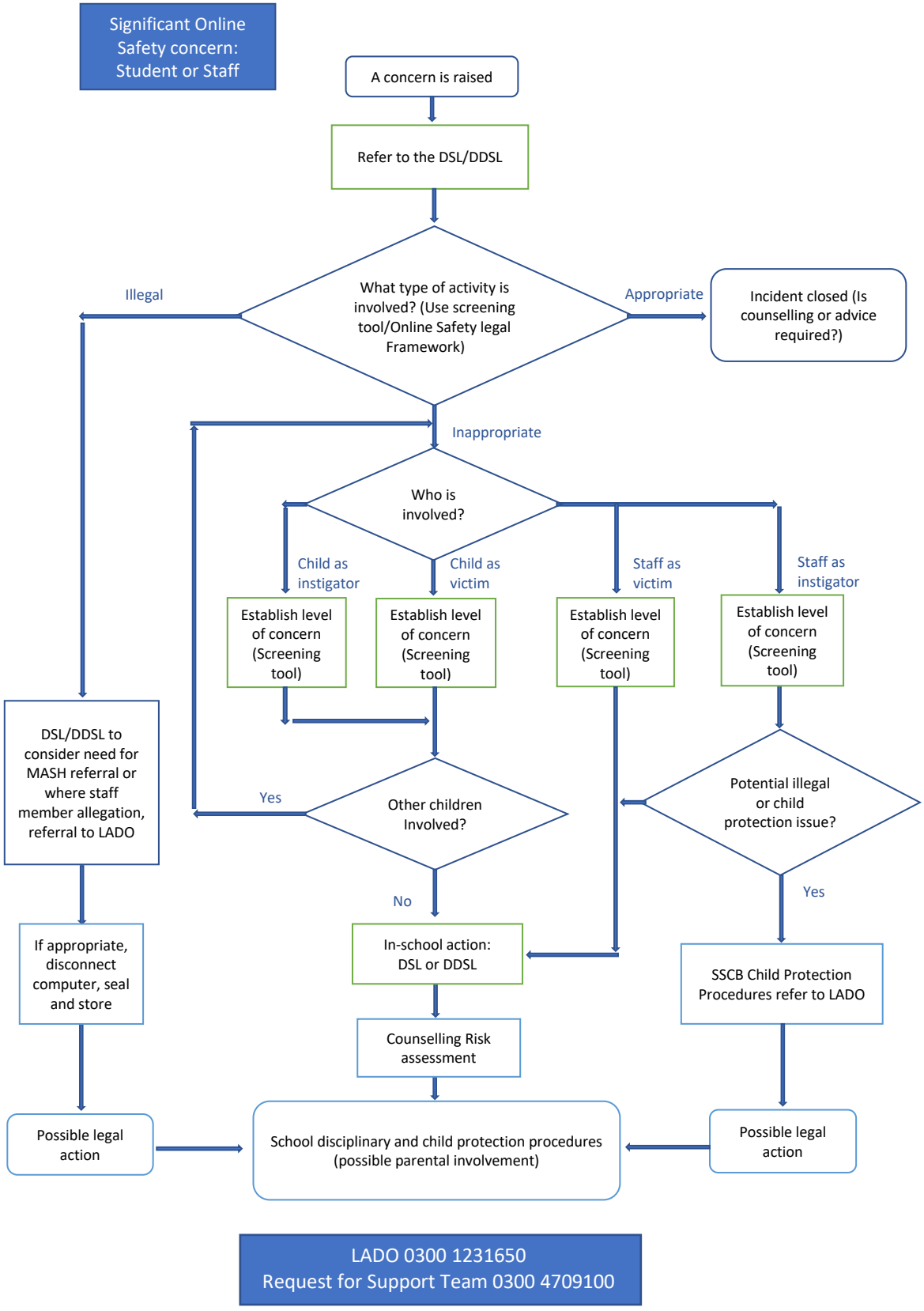
Kidsmart: www.kidsmart.org.uk

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Date Published: May 2019
Expiry Date: May 2021

Appendix 1



Date Published: May 2019
Expiry Date: May 2021