WOODBRIDGE HIGH SCHOOL

e-Safety Policy

Updated: July 2015

Contents

Page

1 Policy Implementation and Oversight 2

2 Teaching and Learning 2

2.1 Why is Internet use important?
2.2 How does Internet use benefit education?
2.3 How can Internet use enhance learning?
2.4 How will students learn how to evaluate content?

3 Managing Information Services 3

3.1 How will information systems security be maintained?
3.2 How will email be managed?
3.3 How will published content be managed?
3.4 Can student images and work be published?
3.5 How will social networking and personal publishing be managed?
3.6 How will filtering be managed?
3.7 How will emerging technologies be managed?
3.8 How should personal data be protected?
3.9 How will videoconferencing be managed?
3.10 How will the school community be protected from extremism and radicalisation?

4 Policy Decisions 6

4.1 How will Internet access be authorised?
4.2 How will risks be assessed?
4.3 How will complaints be handled?
4.4 How should the Internet be used across the community?
4.5 How will Cyberbullying be managed?
4.6 How will Learning Platforms be managed?

5 Communications Policy 8

5.1 How will the policy be introduced to students?
5.2 How will the policy be discussed with staff?
5.3 How will parents' support be enlisted?

6 Incident Flowcharts 9

6.1 Inappropriate activity
6.2 Illegal/Unlawful activity

1. Policy implementation and oversight

- The school has an e–Safety Coordinator. This person liaises with the Designated Child Protection Coordinator as and when the roles overlap.
- The e–Safety Policy and its implementation will be reviewed annually.
- Woodbridge High School's e–Safety Policy has been written by the school, building on government guidance. It has been agreed by the Leadership Group and approved by governors.

2. Teaching and learning

2.1 Why is Internet use important?

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- 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.
- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

2.2 How does Internet use benefit education?

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;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- 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;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with London Borough of Redbridge (LBR) and Department for Education (DfE);
- Access to learning wherever and whenever convenient.

2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Students will be taught what is and isn't acceptable in terms of Internet use and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity.

- 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.

2.4 How will students learn how to evaluate Internet content?

- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching/learning in every subject.

3 Managing Information Systems

3.1 How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not be used without specific permission followed by a virus check. No unapproved software may be executed from portable media.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the school's network will be regularly checked; media files that contravene copyright will be removed.
- The IT Support team will review system capacity regularly.
- Student user areas are provided by the school for students to save files relating to their studies. These are not private storage areas in the same way a student exercise book is not private. The school reserves the right to review the files stored in student user areas as required.

Please refer to the school's data security policy for further information

3.2 How will email be managed?

- Students may only use approved email accounts.
- Students must immediately tell a teacher if they receive offensive email.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an appropriate adult.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- When communicating with students staff should only use the systems provided and managed by the school. These include the Managed Learning Environment and school email accounts.

3.3 How will published content be managed?

- The contact details on the website are the school address, email and telephone number. Staff or students' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. This task will be delegated as appropriate.

3.4 Can student's images or work be published?

- Images that include students will be selected carefully and will not provide material that could be reused.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.
- Students work can only be published with their permission or the parents.
- Students images may be used within the school as part of a learning activity without parental permission (e.g. a video assessment of a drama piece, photos of an experiment taking place), but images will only be stored on school systems for the period of time that the learning activity requires them and deleted afterwards. Images will not be made available to students outside the group specifically engaged in the planned learning activity.

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

- The school will control access to social media and social networking sites from all networked technologies.
- Students will be encouraged to consider the range of risks that are known to be associated with social networking systems. Students will be advised always to limit and carefully manage their privacy settings.
- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Students should be advised to understand the dangers inherent with placing personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should include an understanding of how the background details in a photograph which could identify the student or his/her location.
- Staff official blogs or wikis should be password protected and linked to, or hosted within, the school website with approval from the Leadership Group. Staff should be advised not to run social network spaces for student use on a personal basis.
- Staff should be advised that personal social networking and media systems should not be publicly associated with the school and should understand that bringing their profession and/or their employer into disrepute will result in disciplinary proceedings.
- If personal publishing is to be used with students then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should enable moderation by school staff.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

3.6 How will filtering be managed?

- The school will work with LBR and LGfL to ensure that systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL must be reported to the e–Safety Coordinator.
- If inappropriate sites have been deliberately accessed the school will initiate disciplinary proceedings and/or sanctions as required. If the sites are potentially illegal or a part of a pattern of behaviour the school will involve appropriate safeguarding, law enforcement and local authority professionals.

- The school's broadband access includes filtering appropriate to the age and maturity of students.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.
- The school monitors students' use of the internet through software that flags up keywords that are used in search engines, websites and browsers. A screenshot is captured and recorded as evidence.

3.7 How will emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with students is required.
- Mobile phones should be kept out of sight during the school day. Phones may be used to support learning at the discretion of the teacher. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Should a student or staff member report abusive or inappropriate messages on a personal mobile device the school should (with the owner's permission) photograph the message and follow the school's anti-bullying procedures. Should you suspect that the message is illegal (racist, threatening, etc.) you should isolate the device securely and take advice from local authority, law enforcement and safeguarding colleagues.

3.8 How should personal data be protected?

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

3.9 How will videoconferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information should not be put on the school website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.
- When a videoconference lesson is being streamed live across the internet written permission should be given by all sites and participants.

Users

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the students' age.
- Parents and carers should agree for their children to take part in videoconferences as part of the images permission letter.
- Only key administrators should be given access to videoconferencing administration areas or remote control pages.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

3.10 How will the school community be protected from extremism and radicalisation?

- Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people.
- Staff and students are prohibited from accessing any websites or social network pages that promote such views.
- The school has systems and filtering in place to block extremist material and monitor those who attempt to access it.
- Any persons deemed to be accessing extremist material will be reported to the relevant authorities.
- Refer to the school's policy on extremism and radicalisation for more information.

4 Policy Decisions

4.1 How will Internet access be authorised?

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff must read and sign the 'Digital Technology Handbook' before using any school ICT resource.
- Parents will be informed that students will be provided with supervised internet access, together with guidance of what the school considers to be Acceptable Use.

4.2 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. Neither the school nor LBR can 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.
- Methods to identify, assess and minimise risks will be reviewed regularly.

4.3 How will e–Safety incidents be handled?

- Students are made aware of the various means to report an incident. These include:
    - Informing a parent
    - Informing a teacher (e.g. tutor/year co-ordinator)
    - Online report via the school website
    - Asking a friend to tell an adult
- Staff are made aware of the signs that might indicate abuse, bullying or harassment.

- Incidents will be assessed against the **e-Safety incidents flowcharts** (refer to documents in section 6):
    - If a child or teacher is in immediate danger the school's child protection lead and the police will be contacted.
    - If there is concern about the potential illegality of the issue external advice from appropriate professionals will be sought.
    - Involvement in online extremist activity or concerns about radicalisation of students will be reported to the appropriate authority.
    - Otherwise the school will manage incidents using the schools sanctions, disciplinary and/or anti-bullying policies as appropriate to the situation.
- All e–Safety complaints and incidents will be recorded by the school — including any actions taken.
- All incidents involving staff must be referred to the headteacher.
- Dialogue will be maintained with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguards Unit to review procedures for handling potentially illegal issues.
- Complaints about the school's management of an e-Safety incident will be dealt with under the School's Complaints Procedure.

4.4 How is the Internet used across the community?

- The school will liaise with those local organisations with which it is engaged to establish a common approach to e–Safety.
- The school will be sensitive to internet-related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice. If the external activity negatively impacts on the learning of the students in the school the school will explore appropriate intervention activity.

4.5 How will Cyber bullying be managed?

- Cyber bullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's anti-bullying policy.
- There will be clear procedures in place to support anyone affected by cyber bullying.
- All incidents of cyber bullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyber bullying:
- 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/bullies, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyber bullying are set out in the school's behaviour policy
- The Police will be contacted if a criminal offence is suspected.

4.6 How will Learning Platforms and learning environments be managed?

- LG will monitor the usage of the Managed Learning Environment (MLE) by students and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Students/staff will be advised on acceptable conduct and use when using the MLE
- Only members of the current student, parent/carers and staff community will have access to the MLE.
- All users will be mindful of copyright issues and will only upload appropriate content onto the MLE.
- When staff, students etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

- Any concerns with content may be recorded and dealt with in the following ways:
    a) The user will be asked to remove any material deemed to be inappropriate or offensive.
    b) The material will be removed by the site administrator if the user does not comply.
    c) Access to the MLE for the user may be suspended.
    d) Parents/Carers may be informed
- A visitor may be invited onto the MLE by a member of LG. In this instance there may be an agreed focus or a limited time slot.
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

5 Communication Policy

5.1 How will the policy be introduced to students?

- All users will be informed that network and internet use will be monitored.
- e–Safety is included within the assembly programme through which students will be made aware of current issues and will be reminded of the importance of safe and responsible internet use. This includes participating in Safer Internet Day each February.
- Student instruction in responsible and safe use shall precede internet access.
- An e–Safety module will be included in the ICT schemes of learning, covering both safe school and home use.
- e–Safety training forms part of the Life Studies programme across the Key Stages.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where students are considered to be vulnerable.

5.2 How will the policy be discussed with staff?

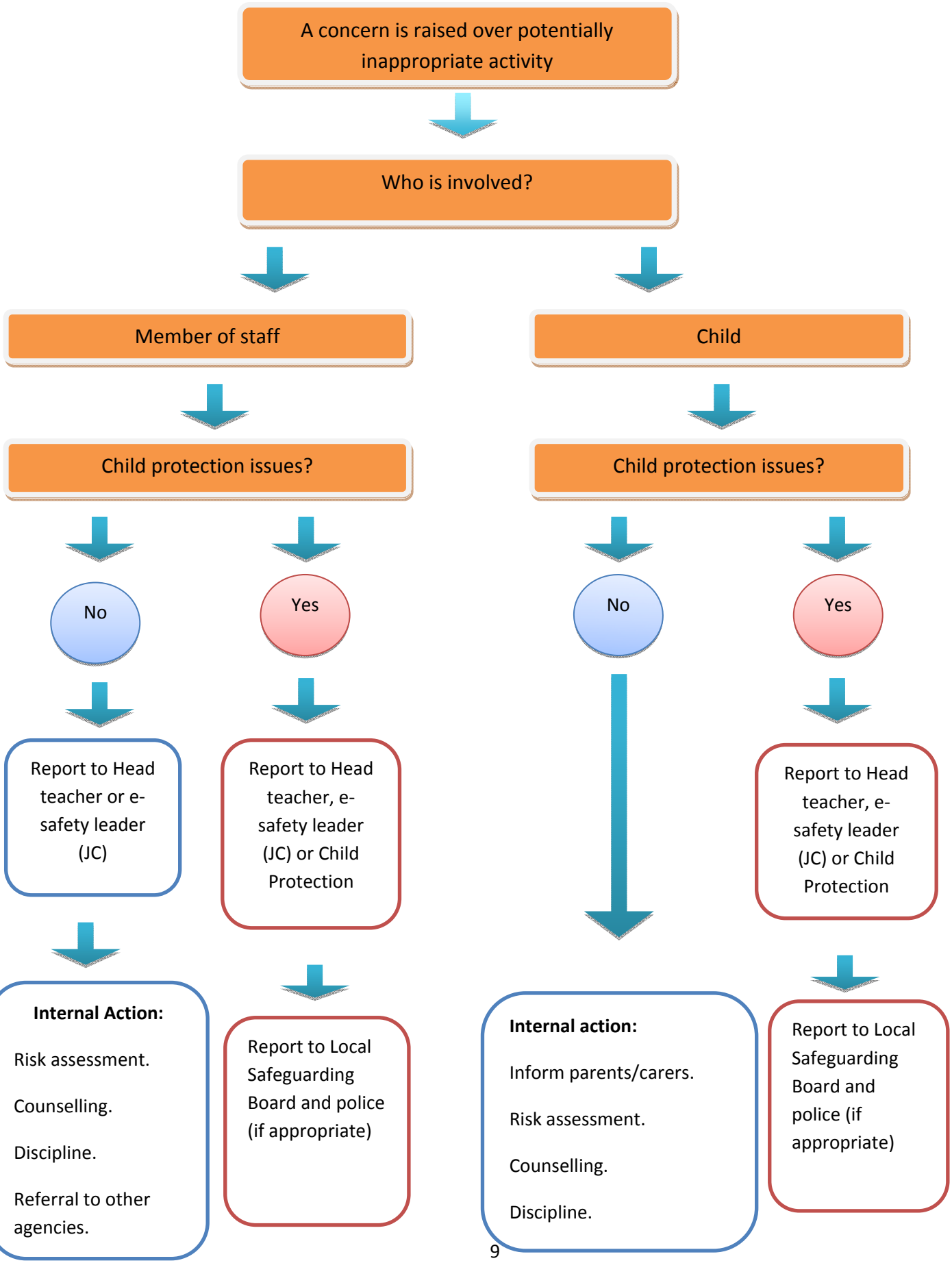
- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and students, the school will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user, Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Leadership Group and have clear procedures for reporting issues.
- Externally-verified, annual staff training covering all aspects of e-safety is provided.
- Staff updates are issued as and when appropriate.

5.3 How will parents' support be enlisted?

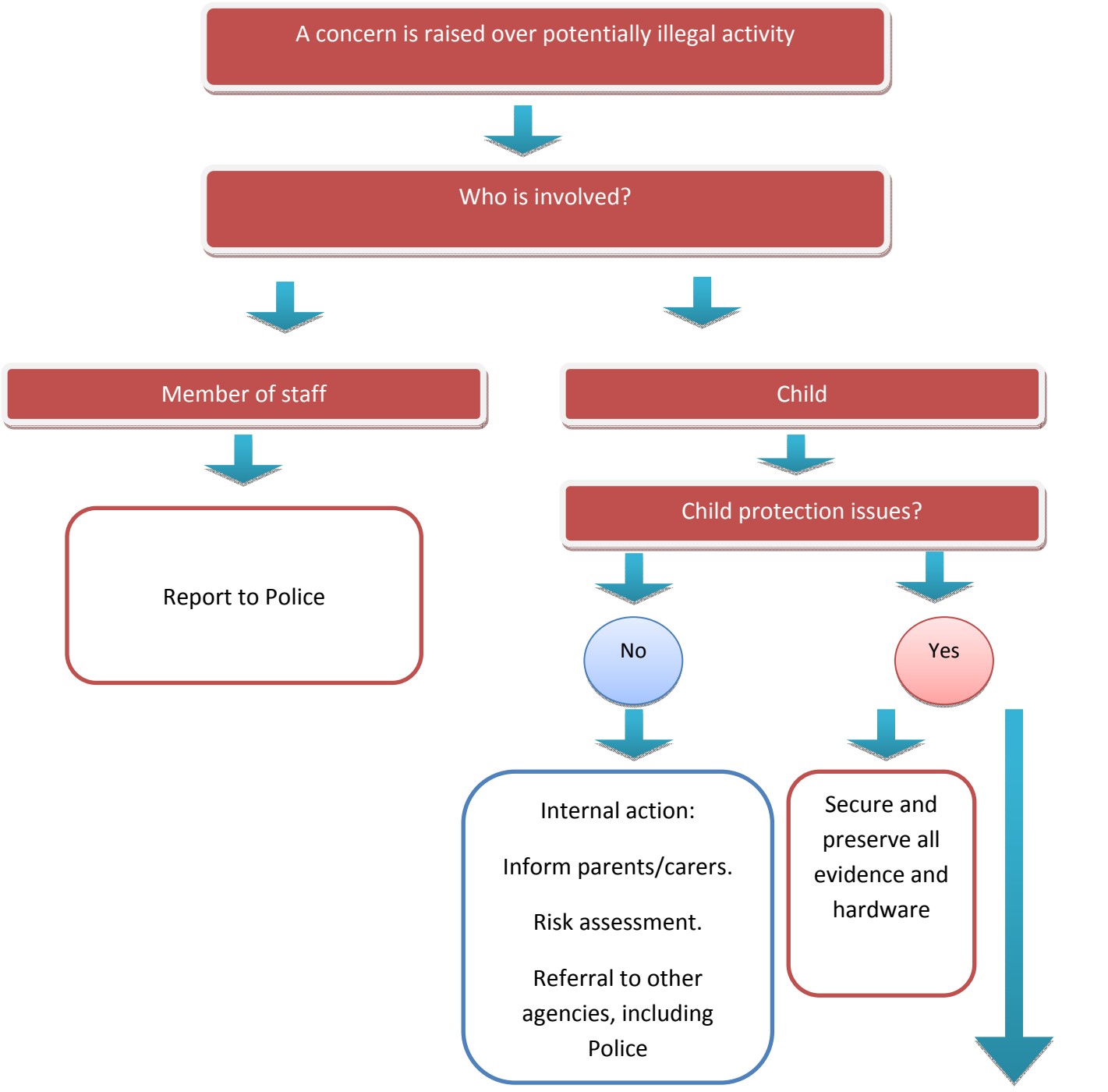
- Parents' attention will be drawn to the School e–Safety Policy in newsletters, via email and on the school website.
- A partnership approach with parents is encouraged. This includes:
    - parent evenings with demonstrations and suggestions for safe home Internet use
    - regular updates and newsletters emailed home.
    - Parentzone magazines set home with the students.
- Externally-verified e-safety training is offered to all parents.

6 Incident Flowcharts

6.1 Inappropriate activity



6.2 Illegal/Unlawful activity



Under no circumstances should any member of staff investigate if illegal activity is suspected. By doing so you may compromise and/or commit further offences.

For example, a member of staff emails you a picture that has been found on another person's computer. The picture looks to be a young person in a state of undress or sexually provocative. You email this to your manager to ask for advice. By sending these two emails, two offences of distributing images of child abuse have been committed.

Policy Prepared by: Mr J. Clifton, Assistant Headteacher: 12 July 2015

Reviewed by the Governors' Scrutiny Group: 15 July 2015, pending formal approval by the F&GP Committee in October 2015

Date of Next Review: March 2016