St Paul's CE Primary School

E Safety Policy

Agreed by Governing Body on:	September 2026
Policy Review Date:	September 2027

1. Policy Statement 3
2. Teaching and Learning 3
2.1 The importance of Internet use 3
2.2 Internet use is part of the statutory curriculum and a necessary tool for learning 3
2.3 Benefits of the Internet to education 3
2.4 Using the Internet to enhance learning 4
2.5 Evaluation of Internet content 4
3. Managing Information Systems 4
3.1 Information system security 4
3.2 E-mail/VLE Messaging 5
3.3 Management of published content 5
3.4 Publishing of pupil/staff images 7
3.5 Management of social networking and personal publishing 7
3.6 Web Filtering 8
3.7 Video conferencing 8
3.8 Emerging Technologies 9
3.9 Protection of personal data 9
4 Policy Decisions 9
4.1 Authorisation to use the Internet 9
4.2 Risk Assessment 10
4.3 E-safety complaints procedure 10
4.4 Community use 10
5 Communications Policy 10
5.1 Policy introduction 10
5.2 Staff sharing of e-safety policy 11
5.3 Parental involvement 11
6 Monitoring and Reporting Procedures 11
7 Whistleblowing 11
8 E-Safety Contacts and References 12
Appendix 1 13
Responsible Use of Computers and Internet 14

1. Policy Statement

.

E-safety is a child protection issue – not an ICT issue.

This policy is to provide clear guidelines, expectations and protection for all members of school, staff and pupils alike, in the use of the Internet and the school's virtual learning platform. The Designated Child Protection officer is also the e-safety officer. They will work closely with the ICT subject leader and ICT Manager to ensure the systems outlined below are in place and monitored. St Paul School's e-Safety Policy has been written by the school, building on the Brighton and Hove model e-Safety Policy and government guidance. It has been agreed by the senior management and approved by governors. The e-Safety Policy and its implementation will be reviewed annually. A copy will be kept in the policies folder on the school intranet and on the parents and e-Safety section of the school website. All members of staff will be made aware of the policy and will be expected to be familiar with it.

2. Teaching and Learning

2.1 The importance of Internet use

- The purpose of Internet and VLE use in school is to raise educational standards, to promote pupil achievement, to promote pupil responsibility in keeping themselves safe in cyberspace, to support the professional work of staff and to enhance the school's management functions.

2.2 Internet use is part of the statutory curriculum and a necessary tool for learning

- Internet and VLE access is available for all students and staff providing they show a responsible and mature approach to its use. It can be withdrawn if and when misused.
- The Internet and VLE is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students and staff with quality Internet access and VLE as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take responsibility of their own safety and security.

2.3 Benefits of the Internet to education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across 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 BHCC and DFE;
- access to learning wherever and whenever convenient.

2.4 Using the Internet to enhance learning

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. For example, older children will be given more opportunity to select appropriate websites for their learning whereas younger children may be given a selected choice or a given website.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

2.5 Evaluation of Internet content

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will be taught to consider the plausibility of websites.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.
- Pupils will be made aware that if they unintentionally come across inappropriate content, they should minimise the screen and report it their class teacher or adult in charge at that time. The e-Safety co-ordinator should be informed either verbally and via email with the URL of the website. The ICT team should be made aware of any such incident.
- E safety lessons will be an integrated feature of the ICT curriculum.

3. Managing Information Systems

3.1 Information system security

- Security strategies will be discussed with the Schools ICT Support team regularly.
- The schools server is backed up via the partner school.
- Anti-Virus protection will be updated regularly by the Schools ICT team. Staff with school laptops need to ensure that either anti-virus protection is installed by the School's ICT technician or they take responsibility themselves to ensure anti-virus protection is put on the laptop.

- The security of individual staff and pupil accounts will be reviewed regularly. Both staff and pupils must be informed of the importance of not sharing passwords and this needs to be reinforced regularly. All staff have individual log ins.
- The administrator account password will be changed if it becomes known.
- Computers should be locked when leaving the room and this should be reinforced
- Computers (including mobile devices) may not be connected to the school network both physically or wirelessly without specific permission – a key is needed from ICT Team
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission followed by a virus check.
- Good practise might be seen as uploading specific files directly to the VLE
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files will not be moved or removed from a shared folder without specific permission
- Personal data will not be stored on school servers without specific permission.
- Software will not be installed/removed from computers without specific permission
- The ICT Team will review system capacity regularly.

3.2 E-mail/VLE Messaging

- Pupils may only use approved school e-mail accounts or VLE messaging in school.
- Pupils must immediately tell their class teacher if they receive offensive e-mail or VLE messages. The class teacher will use professional judgement to decide if the e-Safety co-ordinator needs to be informed. Likewise, if staff receive any inappropriate or offensive e-mail or VLE messages, it must be reported to the e-Safety co-ordinator. Any racist, sexist or homophobic comments will be dealt with in accordance to the school's PSHE policy and logged in the school's e-Safety log held on the school network.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils will have access to individual school email addresses but for many tasks will be able to use a group or class email address.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to external organisations by pupils should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- E-mail sent to external organisations that are work related **must** originate from a school e-mail address. This needs to be reinforced among staff and work e mails should be checked regularly.
- The forwarding of chain letters is not permitted.

3.3 Management of published content

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

3.4 Publishing of pupil/staff images

Pupils also need to be taught the reasons for caution in publishing personal information and images in social publishing sites.

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified in the public section of the school website.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Surnames will be removed from school newsletters and any other relevant letters before being published on the school website.
- Written permission from parents or carers will be obtained before images of pupils are electronically published by the school.
- Written permission from the school should be obtained before pupils or parents/carers publish images taken from the school website or of school events.
- Work can only be published with the permission of the pupil and parents.
- No images of staff will be published on the public pages of the school website.
- Children whose images do not have written permission from parents, will be circulated and made known to all staff.

3.5 Management of social networking and personal publishing

Examples include: Facebook, blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The school will block/filter access to social networking sites in accordance with the Schools ICT Support Teams guidance and filtering system.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils 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 e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space including their VLE homepage. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils 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.
- Should staff became aware of pupil(s) using social networking sites that are not age appropriate, they should remind the pupil(s) of this and advise them on how to keep safe.

- If staff are approached online by pupils (or former pupils) for “friend requests”, they should be declined and if possible the pupil informed in person that it is not school policy. Possible exceptions will be if there is a family connection or family friends. Staff need to be aware of the age restrictions of individual social networking sites.
- Staff must ensure, for their own protection and privacy that any security permissions for social networking sites are set so pupils cannot access them.
- Pupils/staff should be advised not to publish specific and detailed private thoughts.

3.6 Web Filtering

- The school will work with BHCC Schools ICT to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Co-ordinator. Depending on the nature of the site, the school’s Child Protection Officer may also be informed.
- ICT staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies.
- The school’s filtering strategy will be designed by educators to suit the age and curriculum requirements of the pupils, advised by BHCC Schools ICT.
- Sometimes acceptable educational websites are blocked. If you need to use such a website, contact the e-Safety co-ordinator with the URL who will, in turn, inform School’s ICT. The website will be evaluated and if considered safe it will be unblocked. This can take up to 48 hours.

3.7 Video conferencing

- 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. Use over the non-educational network cannot be monitored or controlled.

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils’ age.
- Parents and guardians should agree for their children to take part in videoconferences, probably in the annual return.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- 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.
- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- 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.

3.8 Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff mobile phones should be on silent or turned off for during lesson time.
- Teaching Staff have access to the Teacher2Parent texting system.

3.9 Protection of personal data

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

4 Policy Decisions

4.1 Authorisation to use the Internet

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource. (see Appendix 1)
- Parents and pupils will be asked to sign and return a consent form and Acceptable Use Policy (see Appendix 2) for pupil access in Year 3 onwards. Year 3 class teachers will be responsible for sending out and collecting the signed AUP before handing in to the e-Safety co-ordinator. Any outstanding AUPs will need to be followed up by the class teacher and e Safety co-ordinator.
- Parents will be informed that pupils will be provided with supervised Internet access

4.2 Risk Assessment

- 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 BHCC 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 E-safety complaints procedure

- Complaints of Internet misuse will be dealt with by the e Safety Co-ordinator and senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police School Liaison Officer and contacts at BHCC Schools ICT to establish procedures for handling potentially illegal issues.
- Sanctions within the school discipline policy include:
  - Ensuring a detailed record of the incident and any follow up is put in the school's e safety log held on the Intranet
  - interview/counselling by e Safety co-ordinator a senior member of staff;
  - informing parents or carers;
  - removal of Internet or computer access or suspension from the VLE. for a given period

4.4 Community use

- The school will liaise with local organisations to establish a common approach to e-safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

5 Communications Policy

5.1 Policy introduction

The suggested pupil and parent agreement form should be attached to a copy of the e-safety rules appropriate to the age of the pupil.

Consideration must be given as to the curriculum place for teaching e-safety. Is it an ICT lesson activity, part of the pastoral programme or part of every subject? Or all of these?

Useful e-safety programmes include:

- Think U Know; currently available for secondary pupils. (www.thinkuknow.co.uk/)
- Grid Club www.gridclub.com

- The BBC's ChatGuide: www.bbc.co.uk/chatguide/

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the PSHE and ICT programmes covering both school and home use.

5.2 Staff sharing of e-safety policy

- All staff will be given the School e-Safety Policy and its application and importance explained.
- 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 senior management and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided annually.

5.3 Parental involvement

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use.

6 Monitoring and Reporting Procedures

- Records of all incidents will be reported to the ICT manager, who will keep a record. This record will include the date the incident occurred, who was involved, what action was taken and how it was resolved.
- Where the incident is a child protection concern, it will be recorded as such by the Child Protection Officer (designated person).
- A summary of these records will be shared annually with the governing body, as well as with legitimate agencies as necessary to ensure e-safety. The governor responsible for Child Protection will also view the records on a termly basis and discuss the actions taken in order to safeguard children.

7 Whistleblowing

Where there are concerns about staff conduct with regard to e-safety, then please refer to the child protection policy “allegations against staff.”

8 E-Safety Contacts and References

BBC Chat Guide

http://www.bbc.co.uk/chatguide/
Becta
http://www.becta.org.uk/schools/esafety
Childline
http://www.childline.org.uk/
Childnet
http://www.childnet-int.org
Kidsmart
http://www.kidsmart.org.uk
Digizen
http://www.digizen.org/cyberbullying/film.aspx
Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk
e-Safety in Schools
http://www.clusterweb.org.uk?esafety
Grid Club and the Cyber Cafe
http://www.gridclub.com

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/
Kidsmart
http://www.kidsmart.org.uk/
NCH – The Children’s Charity
http://www.nch.org.uk/information/index.php?i=209
NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
Stop Text Bully
www.stoptextbully.com
Think U Know website
http://www.thinkuknow.co.uk/

Signed …… Chair of Governors. Date:……..

Signed …….. Headteacher. Date:……..

Appendix 1

St Paul's Primary School

Rules for Responsible Computer Use

The school has computers and laptops with Internet access to help your learning. These rules will keep you safe and help us be fair to others.

- I will only access the system with my own login and password.
- I will not access other people's files or try to log on using anyone else's password;
- I will use the computers for school work during lesson time;
- I will not bring in memory sticks or discs from outside school unless I have been given permission and they have been checked by a member of staff for viruses;
- I will ask permission from a member of staff before using the Internet;
- I will only E-mail people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, nor arrange to meet someone, unless my parent or carer has given permission;
- I will report any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit; I will use the Internet responsibly.
- I understand I may be monitored while using a computer in school and the teachers can see what I am doing at any time.

Dear Parents/Carers

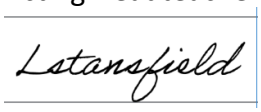
Responsible Use of Computers and Internet

As your child progresses through the school, they will have increased access to the Internet. Please could you take some time to read through and discuss the 'Rules for Responsible Computer Use' with your child before both a parent and child sign the form and return it to the class teacher.

We take e-safety very seriously and are mindful of the problems there are with children gaining access to undesirable materials. We have taken steps, along with the Local Education Authority, to deal with this. Our Internet access is supplied by Brighton & Hove City Council and it has a highly effective, built in filtering system that restricts access to sites containing inappropriate content. All our screens are in public view and normally an adult is present to supervise. No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material.

If you have any further questions please contact me or email admin@stpauls.brighton-hove.sch.uk

Laura Stansfield
Acting Headteacher



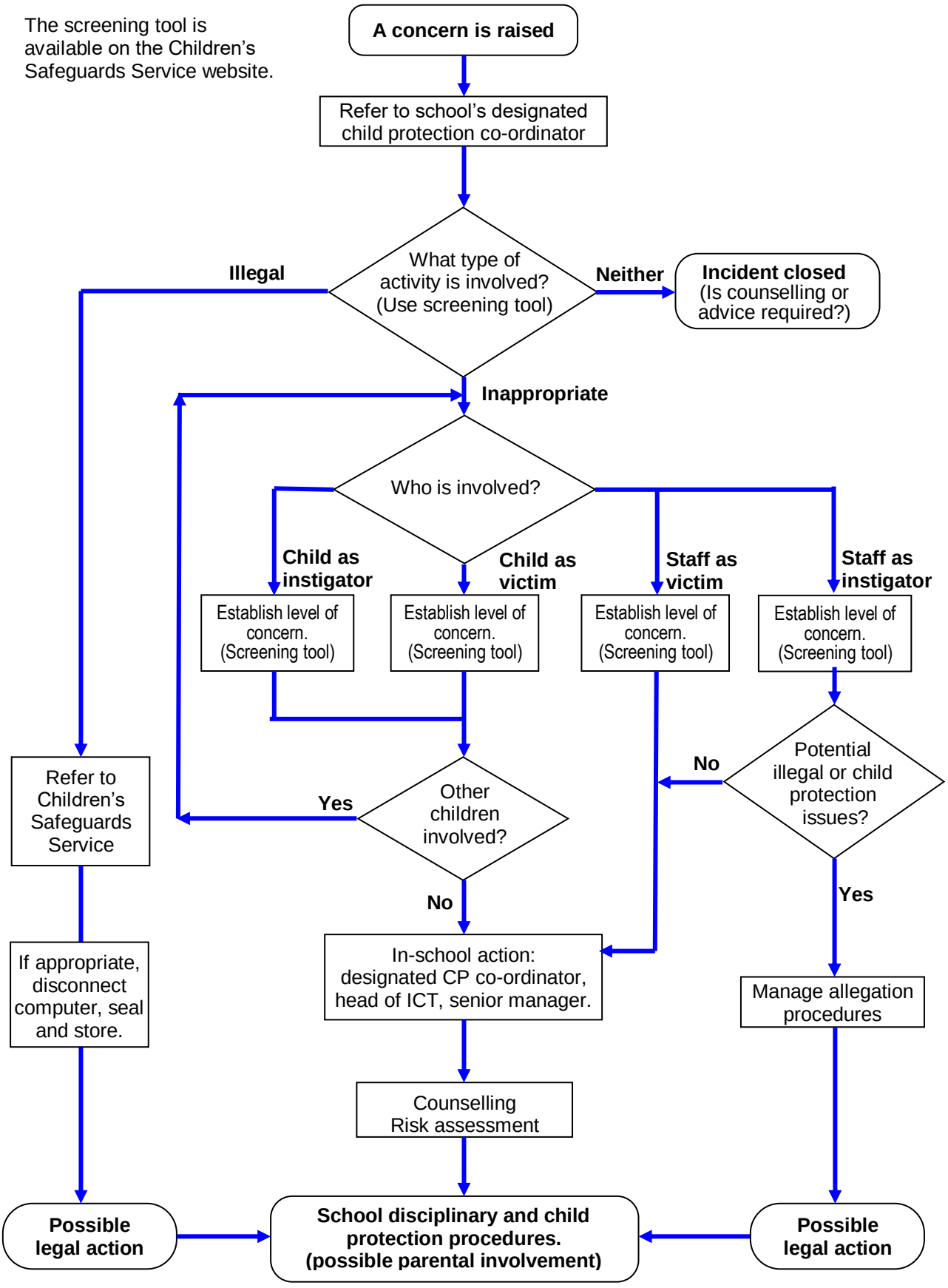
……

Child's Name…… Class……

By signing this we agree to the Rules of Responsible Computer Use

Signed by Child…….

Signed by Parent……

Response to an Incident of Concern

The screening tool is available on the Children's Safeguards Service website.