



E-Safety Policy

Author: Helena Brzeski

Date of issue: January 2020

For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents (*insert others appropriate to your own school needs*).

Safeguarding is a serious matter; at Parkfield Community School we use technology and the internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety, is an area that is constantly evolving and as such this policy will be reviewed every two years or in response to a serious e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Parkfield Community School website; upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy when reviewed and to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of e-safety/computing at the school who will:
 - keep up to date with emerging risks and threats through technology use,
 - receive regular updates from the Head of School in regards to training, identified risks and any incidents,
 - meet with the computing lead to discuss e-safety in school.

Head of School

Reporting to the governing body, the Head of School has overall responsibility for e-safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-Safety Officer, as indicated below.

The Head of School will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to *Helena Brzeski*

The e-Safety Officer will:

- keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use,
- review this policy regularly and bring any matters to the attention of the Head of School,
- advise the Head of School and governing body on all e-safety matters,
- engage with parents and the school community on e-safety matters at school and/or at home,
- liaise with the IT technical support and other agencies as required,
- retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail,
- ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support,
- make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Head of School and responsible governor to decide on what reports may be appropriate for viewing,

- deliver e-safety workshops to parents and monitor e-safety teaching across the PD curriculum.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
 - anti-virus is fit-for-purpose, up to date and applied to all capable devices,
 - Windows and Apple updates are regularly monitored and devices updated as appropriate,
 - any e-safety technical solutions such as internet filtering are operating correctly,
 - filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Head of School,
 - passwords are applied correctly to all users regardless of age, and passwords for staff will be a minimum of 8 characters,
 - the IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff are to ensure that:

- all details within this policy are understood, and if anything is not understood it should be brought to the attention of the Head of School;
- any e-safety incident is reported to the e-Safety Officer (and an e-Safety Incident report is made), or in his/her absence to the Head of School;
- the reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

e-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters and parent workshops, the school will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

Parkfield Community School uses a range of devices including PCs, laptops, Apple Macs, iPads, Chromebooks and Kindles. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use monitoring software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head of School.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. Attachments are scanned before being available to the receiver.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are password protected. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head of School immediately. The Head of School will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed. Children's iPads are not password protected but are monitored and tracked by KRCS.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this e-safety and the staff Acceptable Use Policy; students upon recognition of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Students in Key Stage 2 are permitted to use the school email system, and as such can be given their own email address.

Photos and videos –All parents must sign a photo/video release slip at the beginning of each academic year for staff to be able to take photos of their children and publish them on the school website; non-return of the permission slip will not be assumed as acceptance.

Parents and others attending school events are NOT allowed to take photographs and videos of those events for domestic purposes. For example, parents cannot take video recordings of a school performance involving their child. However, every effort will be made to provide opportunities for parents to take photos of their children at the end of the event.

Social Networking – there are many social networking services available; Parkfield Community School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Parkfield Community School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Officer who will advise the Head of School for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school through the school website.
- Twitter – used by the school as a broadcast service (see below).
- Moodle- used by classes to share learning.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are “comment enabled”, comments are to be set to “moderated”.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner’s permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Head of School. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Parkfield Community School will have an annual programme of training which is suitable to the audience.

e-safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote e-safety.

- The school has a framework for teaching internet skills in ICT/ PD lessons.
- The school provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.
- Pupils are aware of the relevant legislation when using the internet, such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. 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 staff member, or an organisation, such as Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

eSafety Skills Development for Staff

- Our staff receive regular information and training on e-safety. They then promote the 'Stay Safe' online messages in the form of lessons, modeling and guidance e.g. through the use of Moodle.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community (see enclosed flowcharts)
- All staff are encouraged to incorporate e-safety activities and awareness within their curriculum areas
- All staff will receive CEOP training from the e-safety officer.

Managing the School e-safety Messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be introduced to the pupils and staff at the start of each school year.
- E-safety posters will be prominently displayed.
- The key e-safety advice will be promoted widely through school displays, newsletters, class activities and so on.

Acceptable Use Policy – Staff

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Helena Brzeski (school e-safety coordinator) or the Head of School.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils or parents.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Head of School, Computing coordinator or IT manager. Apps may be downloaded on staff iPads for school related purposes without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head of School.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head of School. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature Date

Full Name(printed)

Job title



Acceptable Use Policy – Students



Primary Pupil Acceptable Use Agreement/e-safety Rules

- I will only use ICT in school for school activities and to complete homework.
- I will only use my own school e-mail address on school computers.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will keep my ICT passwords from other children.
- I will only open/delete my own files.
- I will be polite and sensible when using ICT at all times.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- If I accidentally find anything that makes me feel uncomfortable online, I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address to anyone, because this is dangerous.
- I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my e-safety.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

School Council Leader's Signature - _____

Why we Filter the Internet

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the e-safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Very broadly speaking

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

Why do we Filter and Monitor?

Schools filter Internet activity for two reasons:

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice

ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

e-Safety Incident Log

Number:	Reported By: <i>(name of staff member)</i>	Reported To: <i>(e.g. Head, e-Safety Officer)</i>	
	When:	When:	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		Date:	

Smile and Stay Safe Poster

eSafety guidelines to be displayed throughout the school



Be smart on the internet

S SAFE Keep safe by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password. 

M MEETING Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time. 

A ACCEPTING Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages! 

R RELIABLE Someone online might lie about who they are, and information on the internet may not be true. Always check information with other websites, books or someone who knows. 

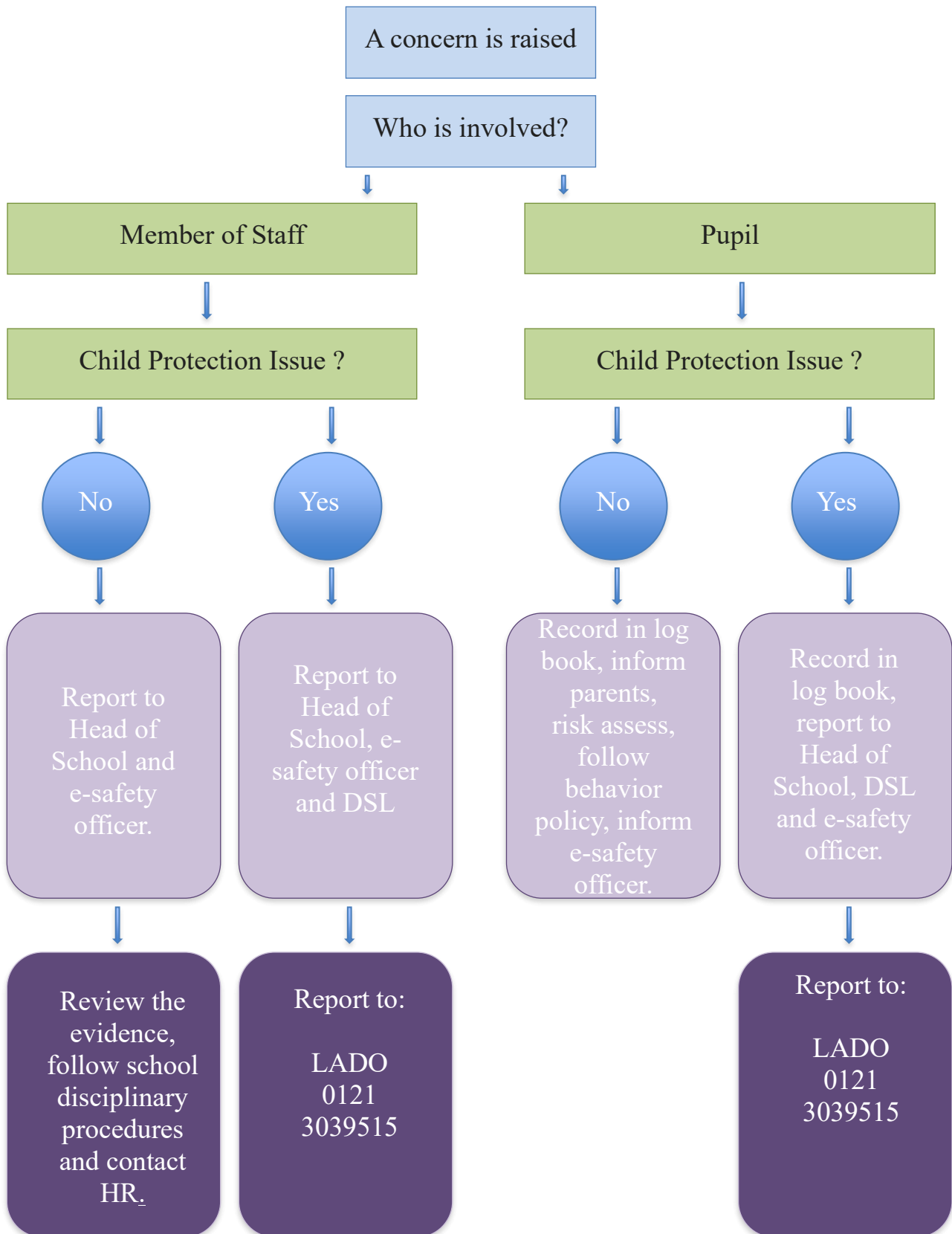
t TELL Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. 
You can report online abuse to the police at www.thinkuknow.co.uk 

www.kidsmart.org.uk

KidSMART  Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world. 

Childnet International © 2020 Registered Charity No. 1091773

Inappropriate Activity Flowchart



If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding

Illegal Activity Flowchart

