North Colchester Primary Collaborative
LOCAL SCHOOLS WORKING TOGETHER

Internet safety Policy and Guidance
Acceptable Use Policy for Staff and Pupils

Refer to:
Behaviour Policy
Child Protection Policy
Anti-Bullying Policy

Review Annually or sooner.
Next Full Review – Autumn 2017

Policy Statement

Policy Governance - Roles/responsibilities

- Governing Body
- Headteacher
- Internet safety Officer
- ICT Technical Support Staff
- All Staff
- All Students
- Parents and Carers

Technology

- Internet Filtering
- Email Filtering
- Encryption
- Passwords
- Anti-Virus

Safe Use

- Internet
- Email
- Photos and videos
- Social Networking
- Incidents
- Training and Curriculum

Acceptable Use Policy (Staff)

SMART Rules for EYFS, KS1 and KS 2

Guidance and other miscellaneous documents

- Why do we filter the Internet?
- Internet safety Incident Log
- Risk Assessment Log
- Inappropriate Use Flowchart
- Illegal Use Flowchart

Policy Statement

For clarity, the Internet 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

NCPC Schools - refers to the following schools: Brinkley Grove Primary School, Friars Grove Primary School, Highwoods Community Primary School, Myland Primary School, Queen Boudica Primary School, St John's CofE Primary School and Willowbrook Primary School.

Safeguarding is a serious matter; at the NCPC Schools we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as Internet safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Internet 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 NCPC schools websites; upon review all members of staff will sign as read and understood both the Internet safety policy and the Staff Acceptable Use Policy.

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 at least annually and in response to any Internet safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Internet 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 Internet safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Internet safety within our school. The day-to-day management of this will be delegated to a member of staff, the Internet safety Officer (or more than one), as indicated below.

The Headteacher will ensure that:

- Internet 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 Internet safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All Internet safety incidents are dealt with promptly and appropriately.

Internet safety Officer

The day-to-day duty of Internet safety Officer is devolved to Helena Jennings.
The Internet 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 Headteacher.
- Advise the Headteacher, governing body on all Internet safety matters.
- Engage with parents and the school community on Internet safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the Internet safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

- Ensure any technical Internet safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical Support.
- Make him/herself aware of any reporting function with technical Internet safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

Computing 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 (or other operating system) updates are regularly monitored and devices updated as appropriate.
  - Any Internet 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 Internet safety officer and Headteacher.
  - Passwords are applied correctly to all users regardless of age **(Note: this will require discussion as to when passwords should be changed.)** Passwords for staff will be a minimum of 8 characters and not relate to family members or pets.
  - The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff/Users

Staff/Users/Governors are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any Internet safety incident is reported to the Internet safety Officer (and an Internet safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the Internet safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this Internet safety policy are fully understood.

All Students

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

Internet 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 the website the school will keep parents up to date with new and emerging Internet safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules and safeguarding procedures in place to ensure that their child can be properly safeguarded. Community users who access school systems / website / behaviour management systems as part of the wide school provision will be expected to sign a Community Acceptable Use Agreement before being provided access.

Technology

The NCPC Schools use a range of devices including PC's, laptops, Apple Mac and iPads. 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 Essex County Council proxy filtering 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 Computing Coordinator, Internet 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 Headteacher. Any items that are deemed inappropriate are to be reported to Essex Broadband Team.

Email Filtering – we use McAfee anti-virus software and Malwares software that prevents any infected email to be sent from the school, or to be received by the school. Our email system is Microsoft Office 365, which has been set up and endorsed by Essex County Council. 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.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. 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 flashdrives/memory sticks) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does not mean password protected.)

Passwords – all staff will be unable to access any device without a unique username and password. Staff passwords will change on a six-monthly basis or if there has been a compromise, whichever is sooner. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed. Staff must ensure the saf-keeping of personal data, minimizing the risk of its loss or misuse

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 Flashdrives/Memory Sticks 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 Internet safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All users/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. All Users (Office, Teaching Staff including Teaching Assistants and Learning Support Assistants, Governors and the PTA) will be given their own e-mail address, solely for the purpose of 'business' communication.

Photos and videos –All parents must sign a photo/video release slip as part of the admission form; non-return of the permission slip will not be assumed as acceptance. The children that do not have permission will be asked at the beginning of the academic year if they wish to be included on the permission form. This will also ascertain if parents give permission for newspaper publication. **The format for both newspaper publication and website will only include the child's first name. It will not give the child's last name.**

Social Networking – there are many social networking services available; The NCPC Schools do not endorse or engage with parents and the wider school community through social networks. Social media services are not permitted for use within the NCPC Schools during the hours of 8:30am and 3:30pm; should staff wish to use other social media, permission must first be sought via the Internet safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

A broadcast service, such as Twitter or Facebook, 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.

Staff Members are strongly advised that being 'friends' with other staff is high risk. Staff members that are also parents are very strongly advised not to be 'friends' with parents and staff.

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 Internet safety incident is to be brought to the immediate attention of the Internet safety Officer, or in his/her absence the Headteacher. The Internet 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, the NCPC Schools will have an annual programme of training which is suitable to the audience.

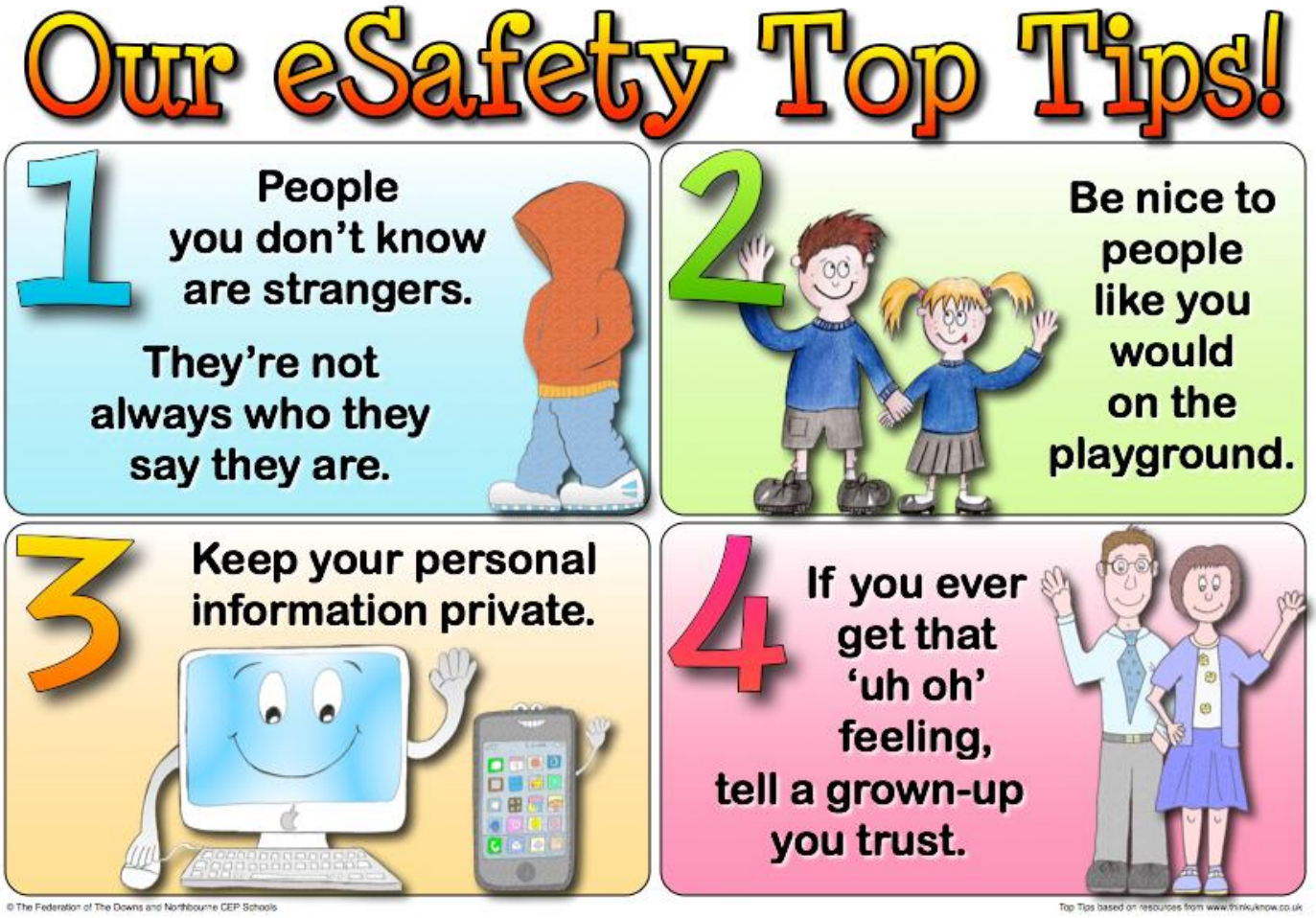
Internet safety for students is embedded into the curriculum; whenever Computing is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. This will take place over the whole academic year using the Computing Curriculum that is suitable for the new National Curriculum 2014.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents. Safer Internet Day will be highlighted as part of an assembly and posters will be placed around the school.

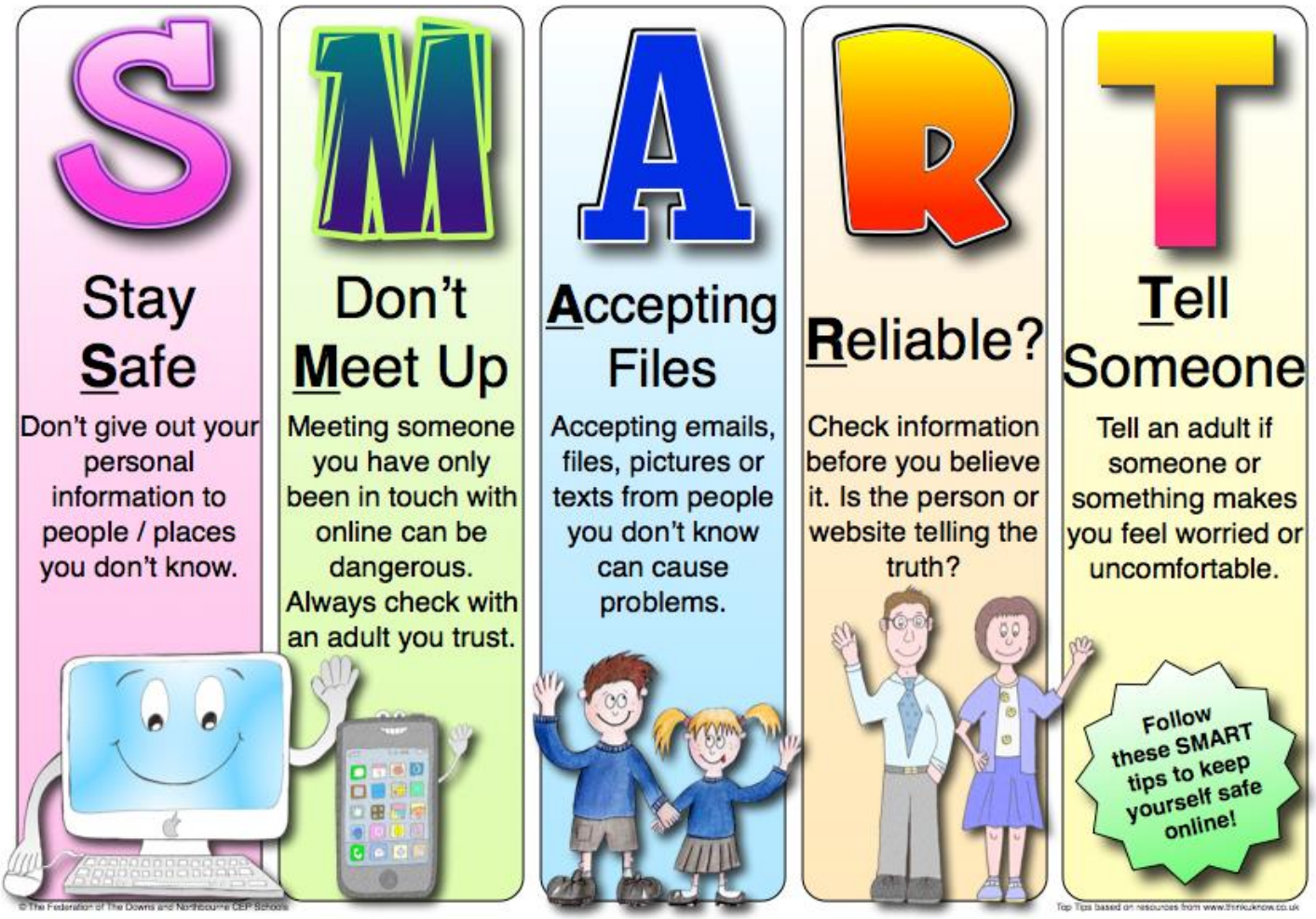
The Internet safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Children's SMART Rules for Internet Use

EYFS and Key Stage 1



KS 2 SMART Rules



Why we Filter the Internet

Introduction

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the Internet 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.

These terms are important; mention to anyone that you are monitoring their Internet use and the immediate vision is of somebody sat at a computer screen watching every move and click; that is simply not the case.

The fact that an Internet filter is in place to filter and monitor activity is of particular importance because you then have questions raised of morality such as, "It's my human right to privacy", "big brother is watching", and others.

Consider CCTV at your school; everybody knows it is there because you can see it and there are (or should be) signs telling people that they are being monitored; everybody knows why it is there whether they agree with it or not.....it is justified for the protection and safety of children and staff whilst in school, and also the protection of the building and its contents.

But what about Internet filtering? How many of your parents know that the online activity of their child may be monitored? How many of your staff know? Importantly, do they know why? Whilst the answer should be "yes" to all, I know that isn't the case and normally with good reason; how do you know what you don't know?

As with many things we do in life it is all about managing expectations, commonly known as justifying ourselves. But it is that justification that gives us precedence for doing something that others may deem controversial.

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 (or should be) 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.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

Managing Expectations

It is the expectations of the user that is particularly important; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however you are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that you are monitoring them. By making reasonable efforts you are working "with" the students and parents, not just merely telling them.

In reality, very few schools actually monitor Internet activity, and neither do local authorities or RBC's (remember, monitor is different to filter). Whether that is right or not is out of scope for this paper, but the fact is you could; in fact Ofsted make clear that schools should be managing their own filter, and this would include monitoring for inappropriate activity, overly-restrictive filtering or otherwise.

Of course, some will disagree with what you are doing, but that is their right and again consent is not a requirement. It is the understanding, not the consent that is important.

Summary

- Filtering is different to monitoring.
- You do not require consent.
- But you must tell users if you do monitor, or if you have the facility to monitor.
- Set user expectations; explain under what circumstances it may be a requirement to monitor.
- Ensure you have a good statement in your Internet safety Policy.
- Ensure you have informed users that Internet use "May be subject to monitoring" in your Acceptable Use Policy.
- Ensure parents are informed, the reason why monitoring may take place, and they sign as read and understood.

North Colchester Primary Collaborative
LOCAL SCHOOLS WORKING TOGETHER

Number:	**Reported By:** (name of staff member)	**Reported To:** (e.g. Head, e-Safety Officer)
	When:	**When:**

Sample e-Safety Incident Log

Review Date:	
Result of Review:	

Signature (Headteacher)		**Date:**	
Signature (eSafety Officer)		**Date:**	

No.	Activity	Risk	Likelihood	Impact	Score	Control Measure	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3		Essex Broadband team e-saftey officer
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6		Internet safety Officer IT Support Essex Broadband team
2.	Blogging/Forum on VLE	Inappropriate comments	2	1	2	Monitoring system with VLE admins. Flagged Messages e-mailed to admin users.	Internet safety Officer Computing Subject Leader
2.	Blogging/Forum on VLE	Using copyright material	2	2	4	Curriculum	Internet safety Officer Computing Subject Leader
3.	Staff laptops	Staff taking laptops home - access to inappropriate/illegal content at home	3	3	9	Acceptable Use Policy	All staff Head Internet safety Officer
4	Data	Staff taking sensitive data home on unencrypted HDD/USB drives	3	3	9	Staff issued with encrypted devices and/or password protection	Internet safety Officer, Issue Password protection/encrypted drives to users
5	Cyber Bullying	E-mails on the VLE, digital communication from outside being brought into school.	2	3	6	Internet safety in the Curriculum	All Staff in Internet safety lesson through curriculum
6	Photographs	Transportation using unencrypted data storage	2	3	6	Refer to AUP	A l l

7	Data protection - misuse	Staff using personal ICT equipment	2	2	4	AUP states to check with HT and/or Internet safety Officer	Head Internet safety Officer
8		Personal Cameras/photo taking devices	2	2	4	Refer to AUP	Internet safety Officer Head
9	Parents taking pictures of other children	At assemblies, School Sports Day, Christmas productions etc then posting on Social Media (not being aware of PPG/LAC/ Vulnerable groups	3	3	9	Parents made aware they are able to take photos of ***only*** their ***own child***, not to post on Social media, but able to e-mail to family etc.	Head Designated Child Safety Officers Internet safety Officer
10	Safeguarding	Safeguarding / LAC / Child Protection	1	3	3	Staff aware of LACs (if applicable) and photographic permissions in school	Des Chi Safety Officers Office Staff Internet safety Officer
		Photographic permissions				Staff aware of Permissions - list in register boxes	Des Chi Safety Officers Office Staff Internet safety Officer
11	Data Protection	Unlocked computers with confidential information (SIMS admin users in front office, class teacher users of SIMS)	3	3	9	Users to refer to AUP, if walking away from machine, lock. If not locked, then lock it.	All users ICT Subject Leaders Internet safety Officer

							Head
		Supply Teacher's having access to school server	3	2	6	Permissions set to limit the access on the school server	PEP Computer's Internet safety Officer Head
12		Staff uploading children's work to Social Media (e.g.Pinterest)	2	2	4	AUP - acceptable use	All Staff
13	Children's Mobile Phones	Theft while on site	2	2	4	Parents inform the school in writing that their children will be bringing a mobile to school. It states in the school documentation that only Yr 5 & 6 should bring in a mobile phone because of walking home alone.	Head Internet safety Officer
14	Children's Mobile Phones	Photographs being taken of staff, pupils / uploaded to social media	3	2.5	7.5	Curriculum Internet safety lesson reminding children that permission must be sought from the Photographee before taking the picture (privacy laws) PSHE Lessons on the effect of Cyber-Bullying Safer Internet Day	ICT Subject Leaders Teaching Staff Curriculum

Risk Assessment

Likelihood: How likely is it that the risk could happen (foreseeability).

Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

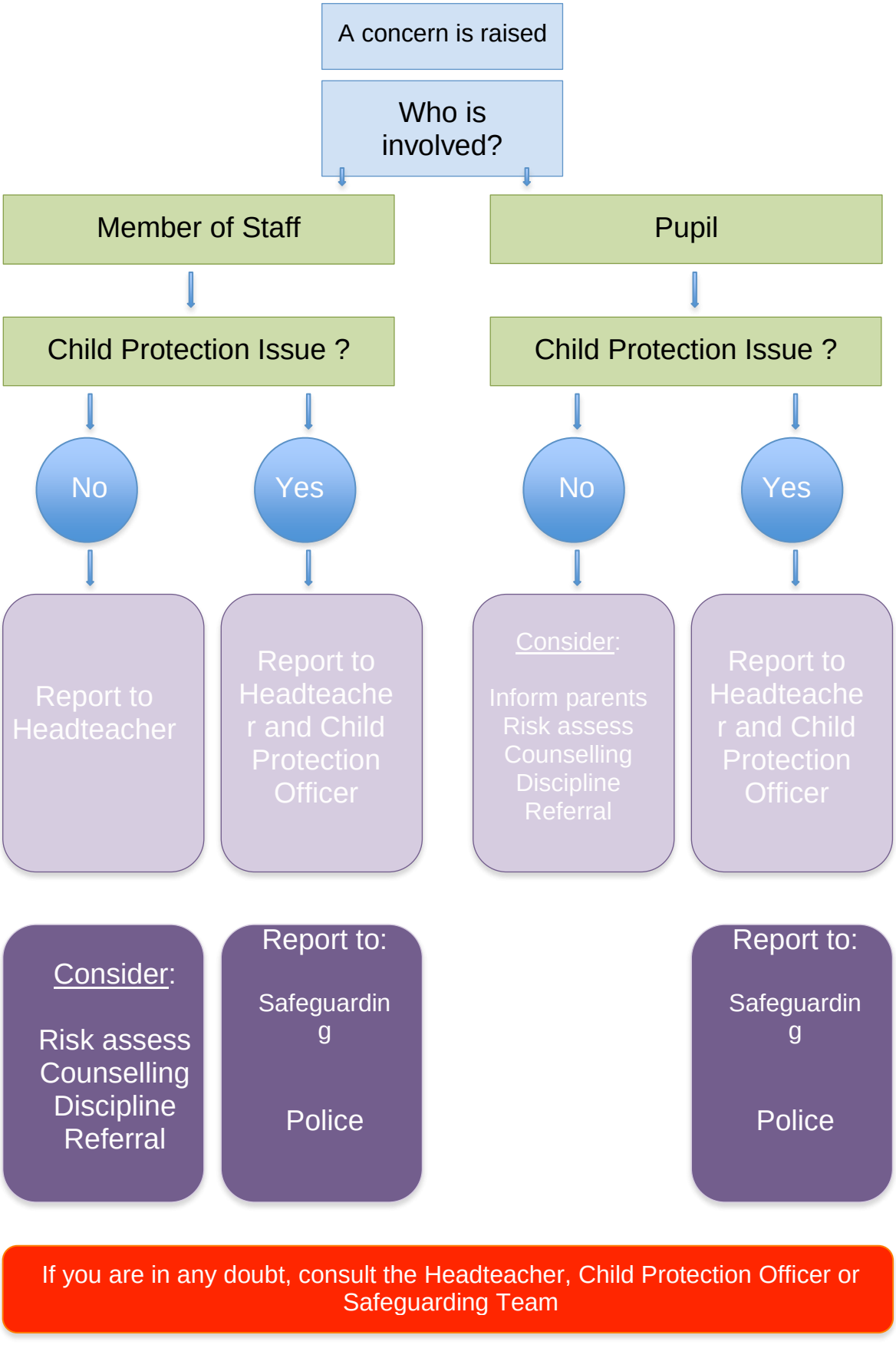
Likelihood and Impact are between 1 and 3, 1 being the lowest.

Multiply Likelihood and Impact to achieve score.

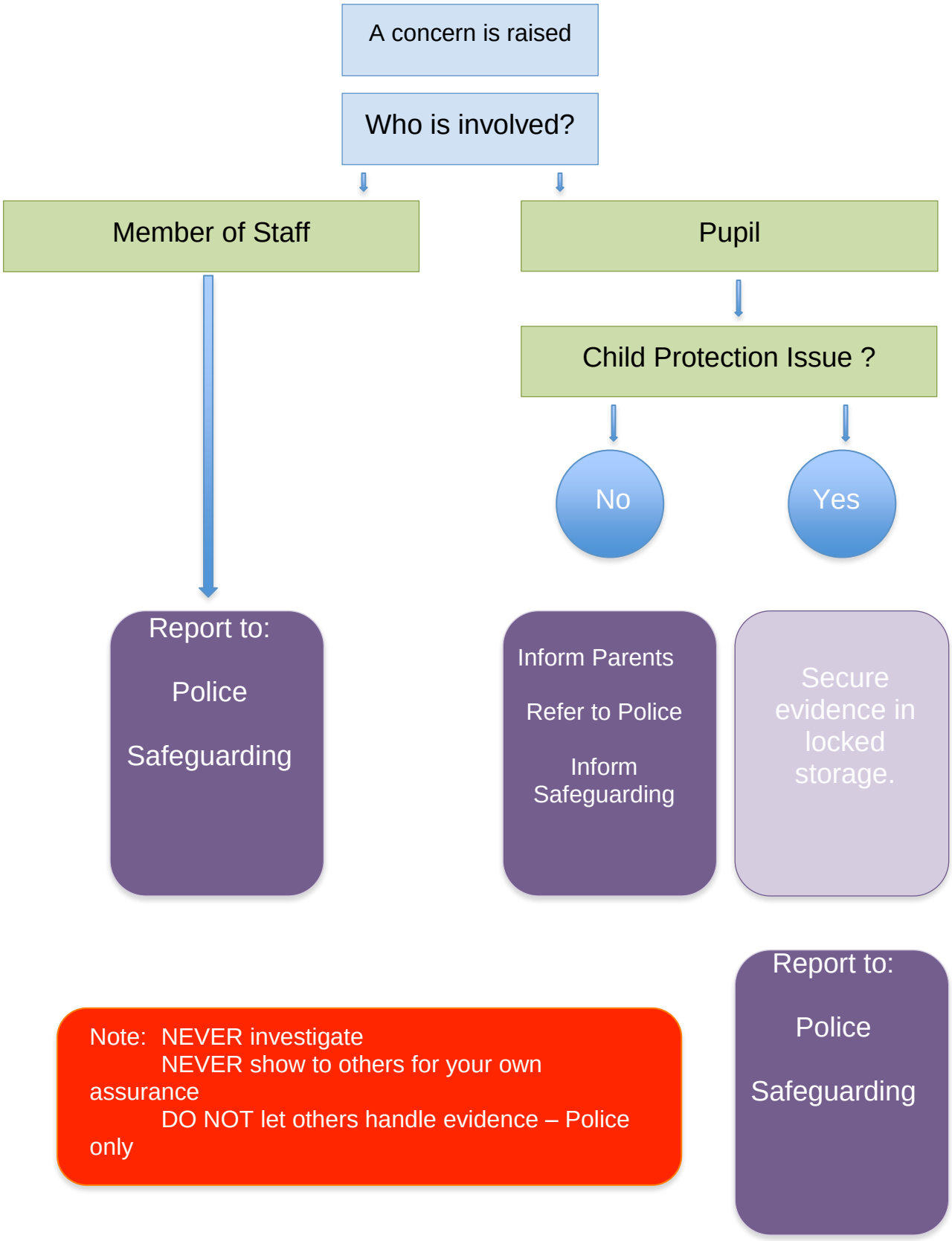
LEGEND/SCORE: 1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.
Final decision rests with Headteacher and Governing Body

Inappropriate Activity Flow Chart



Illegal Activity Flowchart



Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only