BANOVALLUM SCHOOL

E-SAFETY POLICY

Approved by: Behaviour & Welfare Committee

Date Agreed: June 2017

Review Date: Annual

POLICY STATEMENT

This policy should be read in conjunction with the following policies: Behaviour, Safeguarding. For clarity, the e-safety policy uses the following terms unless otherwise stated:

Users	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, hirers of school facilities.

Safeguarding is a serious matter; at Banovallum 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 on an annual basis** or in response to an 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 Banovallum 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 and as such :

  - ○ Mrs Wendy Ireland (Chair of Governors) to have overall responsibility for the governance of esafety at the school who will:
  - ○ Keep up to date with emerging risks and threats through technology use. ○ Receive regular updates from the e-safety officer in regards to training, identified risks and any incidents.
- they will review this policy at least annually
- they will in response to any e-safety incident, ensure that the policy is up to date, covers all aspects of technology use within the school,
- they will ensure e-safety incidents were appropriately dealt with □ and ensure the policy was effective in managing those incidents

HEADTEACHER

Reporting to the governing body, the Headteacher 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 (or more than one), as indicated below.

The Headteacher 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(s) is devolved to Mr Simon Curtis, Miss K Marshall (Deputy).

The e-Safety Officer will:

- Meet every 6 weeks or more often if required with the ICT technical support staff.
- 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 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 local authority, 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 Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT 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 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 Headteacher. • requests for specific sites to be unblocked must be made on the appropriate form to the e-Safety Officer. • passwords are applied correctly to all users regardless of age. • the IT system Administrator password is to be changed on a monthly (30 day) basis.

STAFF	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 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 Headteacher. If you are unsure, the matter is to be raised with the e-Safety Officer or the Headteacher to make a decision. • the reporting flowcharts contained within this e-safety policy are fully understood.
STUDENTS	• **Acceptable Use Policy** - 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, including a student's own device, or services will be dealt with in accordance with the Acceptable Use and Behaviour policies. • 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	play the most important role in the development of their children; as such the school will ensure that • parents must understand the school needs to have to rules in place to ensure that their child can be properly safeguarded. • parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services. • parents of new Y7 intake in September will have 10 days in which to sign the agreement. • parents have the skills and knowledge they need to ensure the safety of children outside the school environment. • through parents evenings and school newsletters the school will keep parents up to date with new and emerging e-safety risks, • parents are involved in strategies to ensure that students are empowered. Banovallum School recognises that parents and other family members will have personal social media accounts which they might use to discuss/share views about school events with friends and family. As a guide, individuals should consider the following prior to posting any information on social media or internet sites about the school, students, staff, or anyone associated with the school. - Will the item identify students or put them at risk of harm? - Is the item defamatory, demeaning or insulting, or likely to upset the child or their parents? - Is social media the appropriate channel to raise or discuss matters about the school or its staff? - Are such comments likely to cause emotional, educational or reputational harm to individuals or the school which could not be justified?

TECHNOLOGY

Banovallum School uses a range of devices including PC's, laptops, Apple Macs. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering	Banovallum School uses BLOXX 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 Headteacher. Forensic Monitors which identifies key words for investigation.
Email Filtering	Banovallum School uses BLOXX 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.
Encryption	Banovallum School uses ESET Deslock Encryption software. All school devices leaving the school that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an unencrypted device. Any breach (i.e. loss/theft of device such as laptop) 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. If it is not possible to encrypt a device, such as a tablet computer, no personal data must be stored on it. Class lists must refer to student only by their initials. An initial from a middle name or an extra letter from a last name may be added to distinguish between students with the same initials.
Passwords	Passwords must: 1. not contain the user's account name or parts of the user's full name or previous password that exceed two consecutive characters 2. be at least eight characters in length 3. contain characters from three of the following four categories: • English uppercase characters (A to Z) • English lowercase characters (a to z) • Base 10 digits (0 to 9) • Non-alphabetic characters (for example, !, $, #, %) Complexity requirements are enforced when passwords are changed or created. 4. Maximum password age of 42 days 5. Password history of 2 (this prevents user from reverting to their last password) 6. Minimum password age of 2 days (This prevents user from circumventing the password history policy)
Anti-Virus	Banovallum School uses ESET Anti-virus soft on all capable devices. This software is updated daily 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 key drives (when handed to the ICT Technical Support Staff) are to be scanned for viruses before use. Such devices are to be used only when there is no alternative method of transferring data.

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 signing and returning their acceptance 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. • use of personal email addresses for work purposes is not permitted. • students are permitted to use the school email system, and as such will be given their own email address. • the email address will be made up of their first initial and surname-e.g. jsmith@banovallumschool.co.uk
Photos and videos	□ All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.
Social Networking	There are many social networking services available; Banovallum 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 Banovallum 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 Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted. □ Twitter – used by the school as a broadcast service (see below). 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” on this service and as such no two-way communication will take place. In addition, the following is to be strictly adhered to: • Permission slips 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 licence which allows for such use (i.e. creative commons).
Notice and take down policy	Should it come to the school’s 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 Headteacher. 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	1. 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, Banovallum School will have an annual programme of training which is suitable to the audience. 2. e-Safety for students is embedded into the curriculum; whenever ICT 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 students' learning 3. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents. 4. The e-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.

ACCEPTABLE USE POLICY – STAFF

All users are reminded that internet and email activity may be monitored. This policy applies to all devices, including personal ones and to all access be it through the school network or other methods such as 3G.

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.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in school, for school use, in accordance with the e-safety policy only. Staff using social networking in or out of school and on a school or personal account, should never undermine the school, its staff, parents or children. Staff should not become “friends” with or ‘follow’ pupils on personal social networks (staff can become social media friends 2 years after a student has left in year 11, this would mean the majority of students would then be 18 years old). Failure to follow these rules may lead to disciplinary action.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support. **Therefore staff must only log on to equipment and resources using their own details.**

Data Protection – If it is necessary for you to take work home, or off site, you **must** ensure that your device (laptop, USB pendrive etc.) is encrypted.

Staff must take all reasonable steps to ensure that their account is not accessed or personal data of students or staff is seen by others. This includes

- not allowing students to work at their computer
- locking the computer when it is unsupervised (ctrl+alt+delete), including when accessing the system remotely (eg from home)

- only accessing the school network remotely when you are certain that no one can see data you are viewing or entering

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without the appropriate consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Adam Taylor (Network Manager) as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety – like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

I have read and understood Banovallum School's e-Safety and Acceptable use policies.

P:\School Policy\e-Safety.doc

NAME :

SIGNATURE : **DATE :**

ACCEPTABLE USE POLICY – STUDENTS

This policy applies to the use of school and personal devices including desktop and laptop computers, mobile phones and tablet computers.
Students will:

- *only use the school network for school purpose. This includes using a 3/4g connection to access the school network or the internet.*
- *not reveal their passwords to anyone, and change them regularly.*
- *not use anyone else's device or allow anyone else to use their device.*
- *not use anyone else's details to log on to any device.*
- *only use their school email address for school purposes. The Student shall make sure that all ICT communications with pupils, teachers or others is appropriate, responsible and sensible.*
- *be responsible for their behaviour when using devices, the Internet and related technologies. This includes resources they access and the language they use.*
- *not download or install software on school technologies.*
- *understand that bullying is unacceptable in any form, and shall not use technology (including their device) to bully, harass, threaten or upset anyone, at school or outside.*

- *not deliberately browse, download, upload or forward material that could be considered offensive and/or illegal.*
- *not browse, download, upload or forward material that could be considered offensive or illegal and will report any potentially offensive and/or illegal material they may accidentally come across whilst on the school network to their teacher immediately. The Student shall not give out any of their personal information including their name, phone number or address.*
- *shall not arrange to meet any individuals whilst on the school network with the device.*
- *ensure that images of other students and/or staff will only be taken, stored and used for school purposes in line with school policy and with their permission. Images shall not be distributed outside the school network without the express permission of the Headteacher.*
- *ensure that their online activity or use of mobile technology, both on school premises and outside of school premises shall not cause the school, the staff, students or others distress or bring the school into disrepute.*
- *respect the privacy and ownership of others' work online at all times.*
- *not attempt to bypass the school internet filtering system. The Student understands that their use of the Internet and other networks is monitored and logged and can be made available to my teachers. The Student understands that these rules are designed to keep them safe and that if they are not followed, school sanctions shall be applied and the Student's parent/carer may be contacted.*
- *be permitted to access the school ICT Network and services up to and including their final day of school at which point their access shall cease.*
- *be responsible for ensuring that their device is not misused. If the device is misused, by the Student or otherwise, the Student understands that the school shall not be held responsible or liable for such misuse.*

Signed (Parent) :

Signed (Student) :

Date :

Letter to Parents:

Dear Parent/Guardian

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet in order to enhance students' learning and provide facilities for research, collaboration and communication. **All users of the school network are reminded that internet and email activity may be monitored.**

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access such sites. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact "scurtis@banovallumschool.co.uk"

Yours Sincerely

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions. I acknowledge that my child has read and understood the school's Acceptable use policy.

Name of Parent/Guardian –

Name of Child –

Signature - Date

E-SAFETY INCIDENT LOG

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

Risk Log

(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	e-Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

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 Bod**

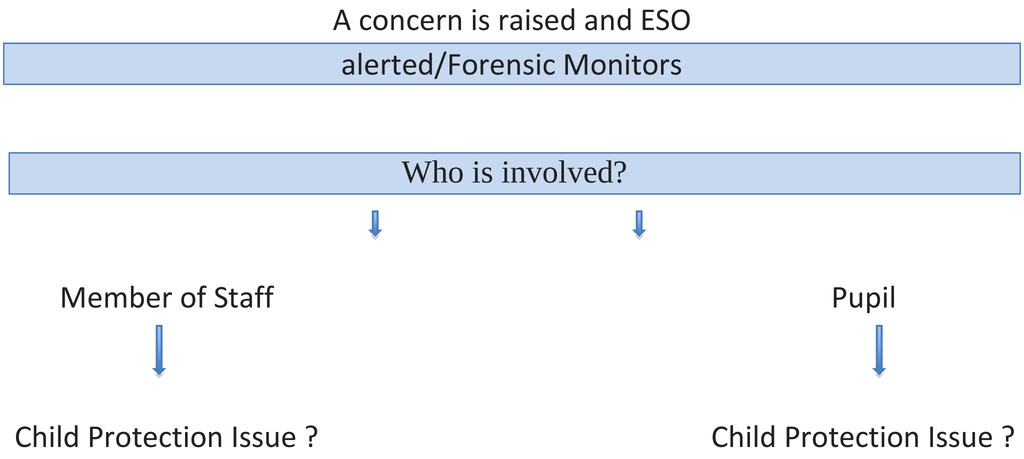
Risk Assessment

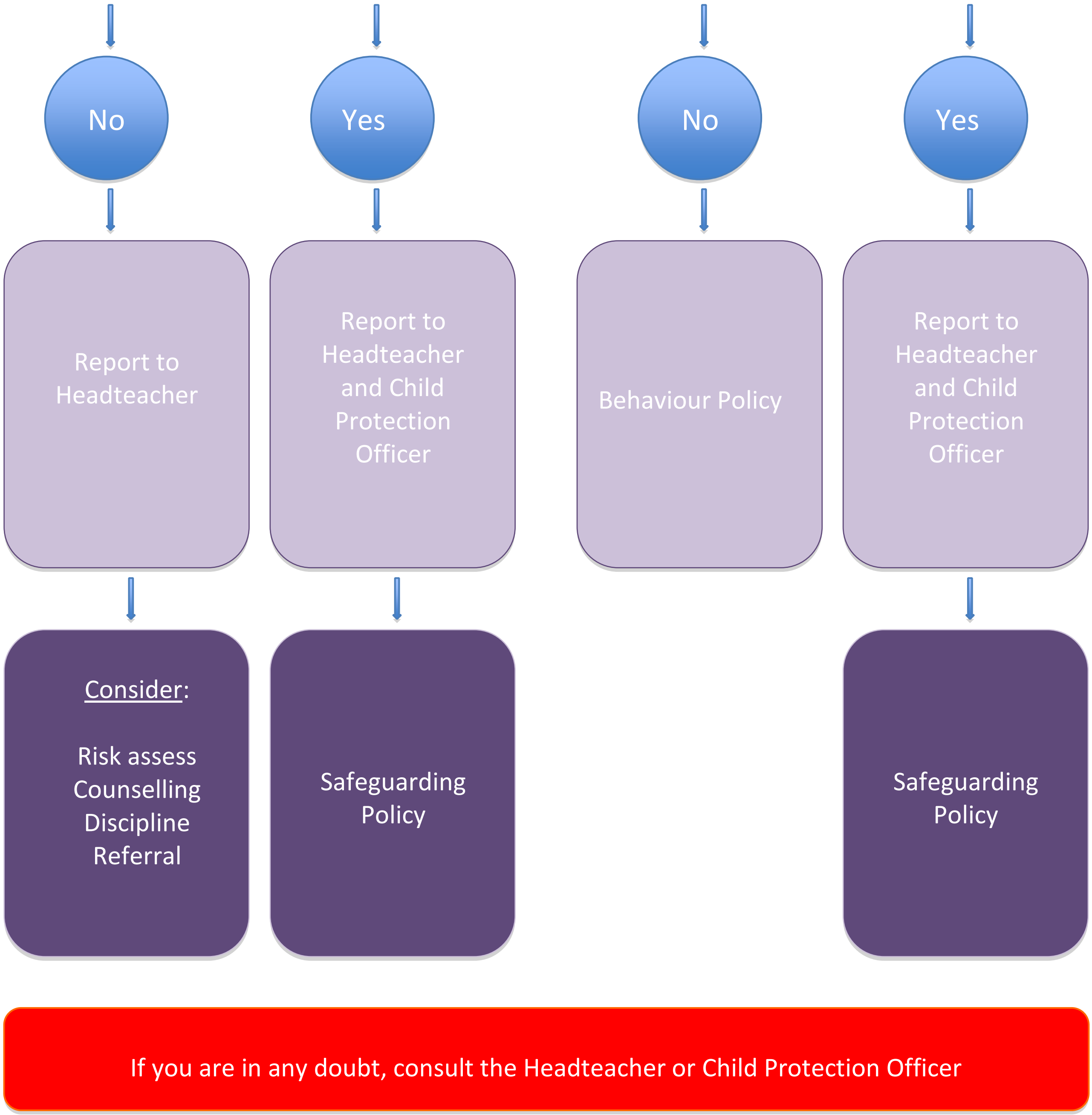
Risk No.	Risk
3	In certain circumstances, students will be able to borrow schoolowned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
LIkelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Approved / Not Approved (circle as appropriate) **Date:**

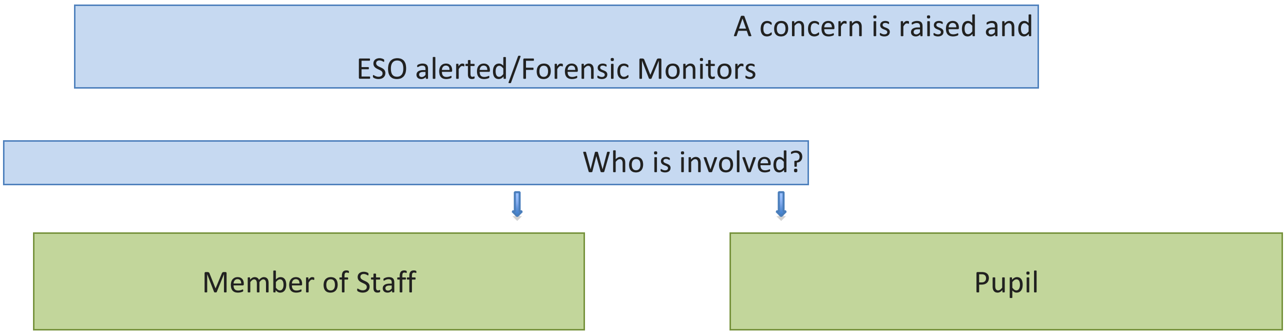
Signed (Headteacher) : **Signed (Governor) :**

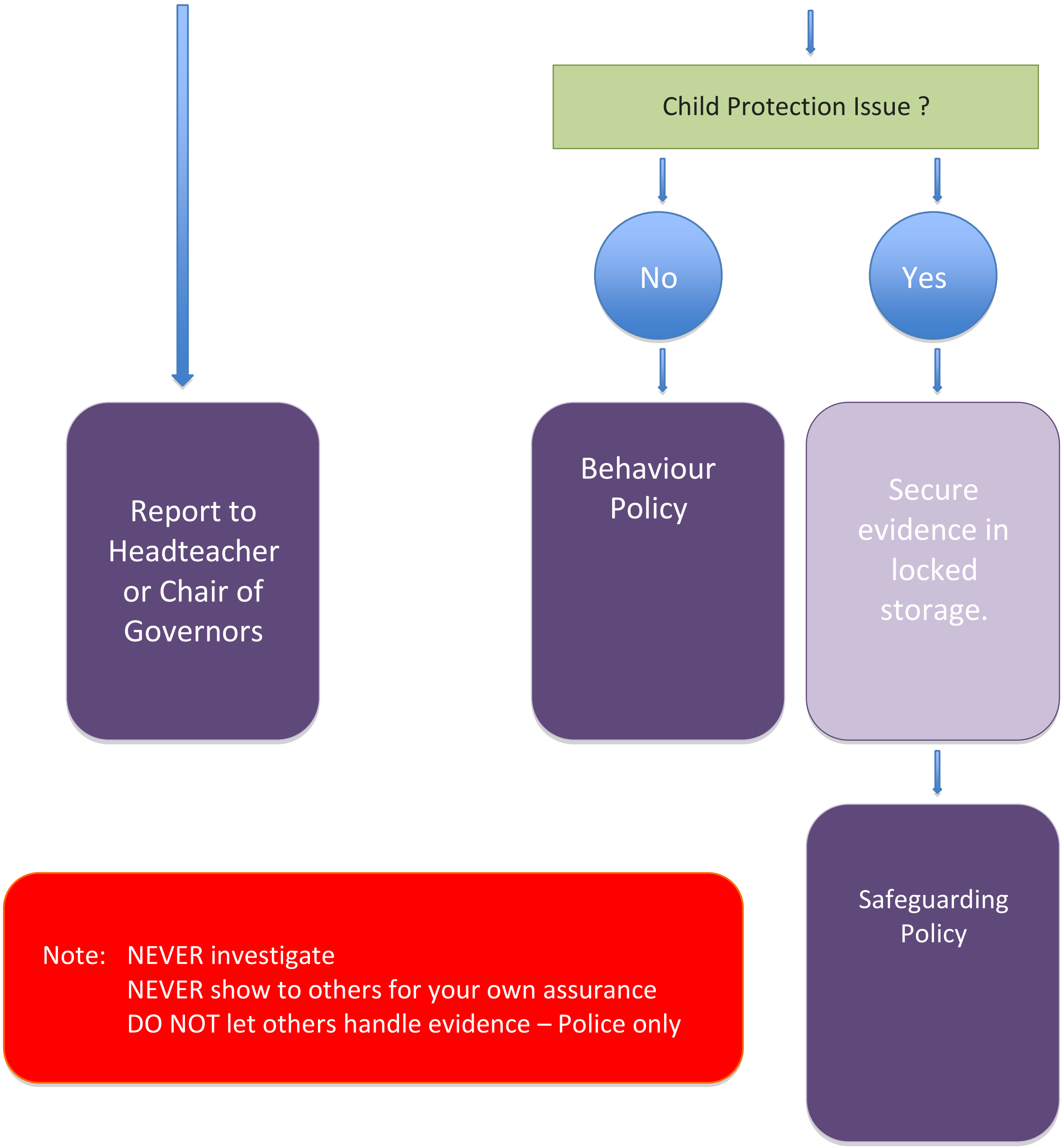
Inappropriate Activity Flowchart




No
Yes
No
Yes
Report to Headteacher
Report to Headteacher and Child Protection Officer
Behaviour Policy
Report to Headteacher and Child Protection Officer
Consider:
Risk assess
Counselling
Discipline
Referral
Safeguarding Policy
Safeguarding Policy
If you are in any doubt, consult the Headteacher or Child Protection Officer

Illegal Activity Flowchart




Child Protection Issue ?
No
Yes
Report to Headteacher or Chair of Governors
Behaviour Policy
Secure evidence in locked storage.
Safeguarding Policy

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