St Vincent's VC Academy
E-Safety Policy

Date policy produced: **September 2019**
Produced by: **St Cuthbert's RC Academy Trust**

Date policy reviewed:
Reviewed by:

Other related school policies that support this E-Safety Policy include:
Whistle Blowing, Anti Bullying, Safeguarding Children/Child Protection, Behaviour, Health & Safety, Data Protection and IT Curriculum

Mission Statement

The motto of our Patron Saint – St Vincent de Paul, "Kindness is the key to all hearts" drives all staff and pupil interactions.

Date	Update
30.1.17	• **How users are notified** • **Filtering & Monitoring**

Policy Statement

For clarity, the E-Safety Policy uses the following terms unless otherwise stated:

Users refers to all staff, pupils, governors, volunteers 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.

Safeguarding is a serious matter and at St Vincent's VC Academy 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 pupil or liability to the school.

This policy is available for anybody to read on the St Vincent's VC Academy website. As part of the induction process, all new staff will receive information and guidance on the e-safety policy, the schools acceptable use policies, plus the reporting procedures.

A copy of this policy and the Pupil Acceptable Use Policy will be sent home with pupils at the beginning of each academic year with a permission slip. Upon return of the signed permission slip, showing acceptance of the terms and conditions, pupils will be permitted access to the school's technology, including the internet.

Policy Governance (Roles & Responsibilities)

The Board of Trustees

The Trustees are 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 e-safety incident 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.

- An appointed Trustee to have overall responsibility for the governance of e-safety across the Trust and will:

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

Headteacher

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, 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. pupils, all staff, senior leadership team, governing body and parents.
- The designated E-Safety Officer has had appropriate training 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 Mrs Joanne Bell.

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarising themselves 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 the 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 themselves 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

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.
    - Passwords are applied correctly to all users regardless of age and should be changed on a termly basis (as a minimum). Passwords for staff will be a minimum of 8 characters. *(Note: you should discuss age-appropriate passwords for pupils and apply this policy).*
    - 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. 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 their 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.

All pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil 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; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils 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 e-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

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

Technology
At St Vincent's VC Academy a range of devices including PCs, laptops and iPads/tablets. In order to safeguard the pupils and prevent loss of personal data we employ the following assistive technology:

How are users notified:

- Staff Inductions - all staff are given an 'Acceptable Use Policy', this must be read, understood & signed. Staff are provided with a copy of the E-Safety Policy.
- Pupils are required to sign: Key Stage 1 'How We Stay Safe on Computers' and Key Stage 2 'Acceptable Use Policy'.

Internet filtering – we use software that prevents unauthorised 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 E-Safety Officer and ICT Technical Support Staff are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

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 or 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 keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the Trust's Data Protection Officer to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does <u>not</u> mean password protected).*

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change if there has been a compromise, whichever is sooner. The E-Safety Officer and ICT Technical Support Staff will be responsible for ensuring that passwords are changed.

Anti-Virus – all capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. ICT Technical Support Staff 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, are to be scanned for viruses before use.

Filtering and monitoring – we filter internet activity for two reasons:

- (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/young people and thereby reduces the liability to the school by making reasonable endeavours to ensure safety.
-

Our internet monitoring arrangements are as follows:

- Our monitoring provider is Smoothwall.
- Internet activity is monitored to ensure policy compliance and prevent pupils and staff accessing inappropriate material.
- Users will be notified that internet activity is monitored through our Acceptable Use Policy for Staff and Pupils informed that activity will be monitored.
- Alerts are recorded, communicated and escalated through the E-Safety Officer (and an e-safety incident report is made) or in their absence, to the Headteacher.

NB: It must be recognised that no monitoring can guarantee to be 100% effective.

Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff upon signing this E-Safety Policy and the Staff Acceptable Use Policy and to pupils upon parents 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. Similarly, use of personal email addresses for work purposes is not permitted.

Photos and videos – working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Social networking – there are many social networking services available; St Vincent's VC Academy 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. DB Learning and the Open Futures website are permitted for use within St Vincent's VC Academy and have been appropriately risk assessed; should staff wish to use any other form of 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.

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 pupil 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 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 their 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.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our academy follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

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, St Vincent's VC Academy School will have an annual programme of training which is suitable to the audience.
E-Safety for pupils 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 pupil's learning. Each year group has devoted time each year to e-safety and a long term plan is in operation, using CEOP resources. All children are involved in E-Safety Week each year. Rules for responsible internet use are displayed throughout the school.
As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

Prevent – St Vincent's VC Academy will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which takes into account the needs of pupils.

When concerns are noted by staff that a pupil may be at risk of radicalisation online then the Child Protection Co-ordinator will be informed immediately and action will be taken in line with the school's Child Protection/Safeguarding Policy

Safety in a Digital World: Guide for Parents/Carers

- **You were taught road safety,**
- **You were taught rail safety,**
- **You were taught to play safely.**

But now we are in the 21st Century and your children need to be taught e-safety.

Children access the Internet on:

- **Computers**
- **Mobile phones**
- **Games consoles**
- **Music systems**
- **And they play games online with friends and *strangers***

They blog, chat, enter competitions, social network, email, watch TV online, download and upload information. They are creative at making music, making films and making web content.

Are you worried about their safety whilst accessing the internet?

This leaflet will provide you with some basic information to help you feel more confident in supporting your child to be e-safe.

The Benefits of Digital Technology

There are many benefits of having access to digital technologies. Here are some of them:

- Used effectively, these can improve children's achievement.
- Using them at home and at school develops skills for life.
- Children with supportive and involved parents and carers do better at school.
- Children enjoy using them.
- Using technologies provides access to a wider and more flexible range of learning materials.

Staying Safe

You can make a huge difference if you talk to your child about how they use digital technology, let them know you are there to guide them and pass on essential safety advice. Here are some do's and don'ts:

- Do remind them that everyone they meet online is a stranger even though they might seem like a friend.
- Do encourage your child never to meet up with someone they make friends with online. But if they do then make sure they take along an adult you trust and to meet in a public place.
- Do explain that they shouldn't accept emails or open files from people they don't know.
- They may contain viruses, nasty messages or annoying links to things you don't want them to see.
- Do be aware that your child may as likely be a cyberbully as be a target of cyberbullying. Be alert to your child seeming upset after using the internet or their mobile phone.
- Do talk to your child so they know they can come to you if they run into any problems. Your continued involvement is the best way of keeping your child safe.
- Do make clear what content and behaviour is acceptable, check that sites are age appropriate.
- Do give your child the knowledge and skills to build up resilience to the things they find online, help them to play and learn safely.
- Do consider using filtering software and agree ground rules about what services you are happy for your child to use.
- Do know how to complain.
- Don't allow them to give out personal information. That means full name, home or school address, telephone number or personal email or mobile number.
- Don't allow your child to access inappropriate sites.

If you want to find out more

A guide for parents about the potential dangers facing their children on the internet, plus advice on what parents can do to help counter these hazards:
www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety

Find the latest information on websites, mobiles and new technology. Find out what's good, what's not and what you can do about it: www.thinkyouknow.co.uk

The UK Council for Child Internet Safety (**UKCCIS**) brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Safer Children in a Digital World consultation: www.dcsf.gov.uk/ukccis

Childnet International is a non-profit organisation working with others to help make the internet a great and safe place for children: www.childnet-int.org

The Child Exploitation and Online Protection Centre (CEOP) works across the **UK** tackling child sex abuse and providing advice for parents, young people and children about internet safety: www.ceop.gov.uk

Or call 01482 616719 for further help and guidance.

Teach your child the internet safety code, Click Clever, Click Safe.

- **Zip It** – Keep your personal stuff private and think about what you say and do online

- **Block It** – Block people who send you nasty messages and don't open unknown links and attachments
- **Flag It** – Flag up with someone you trust if anything upsets you or if someone asks to meet you online

St Vincent's VC Academy
Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the E-Safety Policy. Once you have read and understood both you must sign this policy sheet.

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 not allowed on school premises and social network sites are blocked via the school internet. When making use of social networking off premises staff need to ensure they do not publish their association with the school (e.g. in their status), should never undermine the school, its staff, parents or children nor discuss any school matter. Staff should not become "friends" with parents or pupils on personal social networks.

Staff must set and maintain my profile settings on social networking sites to maximum privacy and give access to known friends only. Staff must not access social networking sites for personal use during school hours or using school equipment. If staff experience any derogatory or slanderous comments relating to the school, colleagues or own professional status, they will take screenshots for evidence and escalate to the E-Safety Officer.

Use of email - 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, pupil or IT support.

Data protection - if it is necessary for you to take work home or off site, you should ensure that your device (laptop, USB, pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal use of school ICT - any staff who have been issued with school laptops/iPads/tablets as part of their role in school (namely teachers, TAs and the Business Manager) have permission to use the devices at home and this may include personal use. However each member of staff has a responsibility to ensure this device is password protected and appropriately used both inside and outside school.

Mobile phones and cameras - Staff must not use mobile phones in rooms where children are present, including those where children are cared for. It is appropriate to take photographs of children to capture a curriculum activity or a celebration of school life using school equipment providing we have permission to do so from the parents. Staff must not, however, use their personal mobile phone, camera (still or moving images) or other devices to take, edit or store images of children from this school. **(Also referenced in Safeguarding Children and Child Protection Policy 2016).**

Purchasing via the internet - as online purchases become more common and offer best value, staff may wish to raise orders or make small purchases via the internet. In this instance the same ordering requirements are in place as shopping in person. If the amount is below £25 then staff can make a purchase from their personal accounts using a debit card, after obtaining Headteacher authorisation, and present the receipt to the administration staff to enable them to be reimbursed through the petty cash system. For purchases greater than this amount the normal ordering procedures apply and staff should request the administration staff to raise an order where possible.

Images and videos - you should not upload onto any internet site, service images or videos of yourself, other staff or pupils without 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 ICT Technical Support Staff and the E-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the ICT Technical Support Staff 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.

A reminder to staff - the internet provides students with access to a wide-range of content, some of which is harmful. Extremists use the internet, including social media, to share their messages. The filtering system used at St Vincent's VC Academy blocks inappropriate content, including extremist content. Where staff, pupils or visitors find unblocked extremist content they must report it to a senior member of staff.

NAME :

SIGNATURE : **DATE :**

St Vincent's VC Academy
Acceptable Use Policy – Pupils (with parents)

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand – that some people on the internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (Pupil):

Date:

KS1 (for use in class)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer.
- I will not tell my friends my password or log-on.
- I will only use activities that an adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

Class: _____ **Date:** __ /__ /__

Class signatures:

KS2 Pupil Acceptable Use Agreement (for use in class)

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at or change, other people's files without their permission.
- I will keep my log-ins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit internet sites that I know to be banned by the school.
- I will only e-mail people I know or a responsible adult has approved.
- The messages I send or information I upload, will always be polite and sensible.
- I will not open an attachment or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: *Date:*

(For use with whole KS2 class)

Keeping Safe: Stop, Think, Before You Click!

Class: _____ Year: ____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me.

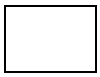
I understand these rules are there to help ☐ keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, internet, email, online communities, ☐ digital cameras, video recorders and other ICT in a safe and responsible way.

☐

I understand that the school can check my computer files, and the internet sites I visit and that if they have concerns about my safety, that they may contact my parent / carer.

Pupil's signatures:



_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,
_____, _____, _____, _____,

Date: ___/___/___

St Vincent's VC Academy
E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Headteacher, 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:**	

St Cuthbert's Roman Catholic Academy Trust

Template 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 Body

Example Risk Assessment

Risk No.	Risk
3	In certain circumstances, pupils will be able to borrow school-owned 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; pupils 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 ICT Technical Support Staff
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using smoothwall 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 pupil 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 pupil 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, pupils are up to date and aware of the risks.

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

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

Reporting Log
Group .....

Date	Time	Incident	Action taken		Incident Reported by	Signature
			What?	By whom?		

Response to Risk Flowchart

Response to and Reporting of an E-safety Incident of Concern