Annex I

E Safety
Wheeler Primary School
School Specific Information

1. Headteacher

   Mrs Claire Mudd
2. Chair of Governors

   Mr Steve Jones
3. Designated Governor for Safeguarding

   Mr Paul Lum
4. Designated Teacher for Safeguarding

   Mrs Claire Burrows
5. Designated E Safety Lead

   Mr Lewis Richards
6. Trust Safeguarding Lead
   - Suzanne Wilson contact Swilson@hcat.org.uk

E-Safety policy

Hull Collaborative Academy Trust

Date issued: March 2019
Ratified by the Trust Board:
Review Date: March 2022

Other related academy policies that support this E-Safety policy include:- Anti-Bullying, Attendance, Behaviour, Child Protection, Data Protection, ICT, PSHE, Staff Code of Conduct & Whistle Blowing

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 academy e.g. parent, guardian, carer.

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

Safeguarding is a serious matter; in HCAT Schools 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 academy 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 academy.

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 Pupils 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 and acceptance of the terms and conditions, pupil will be permitted access to academy's technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our academy 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 academy, 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 at the academy 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 e-safety within our academy. 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. pupils, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer(s) 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 the school, see named individual in appendix A.

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise 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, 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 academy (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

The technical support staff is 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 *(Note: this will require discussion as to when passwords should be changed (I recommend termly at an absolute minimum)).* Passwords for staff will be a minimum of 8

characters. *(Note: you should discuss age-appropriate passwords for pupils and apply within this policy).*

- The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff

Staff members 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 academy 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 academy 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 academy 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 academy needs have to 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

HCAT Schools use a range of devices including PC's, laptops and iPads. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use a hardware based filtering system (Smoothwall – provided via a proxy through ERYC) 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.

Whilst it is essential that Governors, ICT Coordinator, e-Safety Officer and IT Support ensure that appropriate filters and monitoring systems are in place, we are careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Our Governors, ICT Coordinator, e-Safety Officer and IT Support ensure that children are safe from terrorist and extremist material when accessing the internet in schools – this material is blocked through our filtering system. Any issues with regards to extremist material is brought to the attention of the E-safety officer & Headteacher.

Filtering will also attempt to block pupil's ability to be contacted by people external to HCAT Schools and the academy organization. Platforms that the school introduce, such as blogging will be moderated by teaching staff at all times to ensure any communication is positive and safe. Any communication which is deemed to be a concern will not be accepted by teaching staff.

THE MARVELL COLLEGE ONLY

Mobile Technology - the college recognises that 3G and 4G technology does not go through our web filtering system. As such we educate the pupils via PSHE lessons and assemblies about the importance of staying safe online. With the Acceptable User policy, we aim to minimise the risks to our pupils. Any use of mobile technologies (e.g. 4G, 3G or mobile internet services) to intimidate, threaten or cause harm to others will be taken seriously, and if appropriate, action taken, in accordance with the college's behaviour policy.

ALL PRIMARIES

Mobile Technology – as the proliferation of mobile technology continues to expand, HCAT Primary Schools will continue to ensure these devices offer the same level of filtering protection as more traditional technology. No child is allowed a personal device on site during the school day. All mobile devices brought to school by the pupils will be kept in the office until the end of the school day.

Email Filtering – we use the in-built Microsoft Office 365 software that aims to prevent 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. Pupils can only receive and send emails internally to those addresses that end @XXXX.hull.sch.uk or equivalent academy email address.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 2018) 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 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.
(Note: some devices may not be password enabled therefore you may need to indicate this).

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; pupils 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. 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; The Trust 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 HCAT 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.

- Blogging – used by staff and pupils in school.
- Twitter – used by the school, mainly 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. However, some parents, schools or businesses will be "followed" or "friended" on these services to allow two-way communication.

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 academy 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 academy's attention that there is a resource which has been inadvertently uploaded, and the academy 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.

Searching devices

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.

Where the person conducting the search finds an electronic device they may examine any data or files on the device if they think there is a good reason to do so. Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The member of staff must have regard to the following guidance issued by the
Secretary of State when determining what is a "good reason" for examining or erasing the contents of an electronic device: In determining a 'good reason' to examine or erase the data or files the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

If inappropriate material is found on the device it is up to the teacher to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

Sexting - All school staff should be aware that behaviours linked to sexting put a child in danger. Governing bodies should ensure sexting and the school's approach to it is reflected in the child protection policy.

Curriculum - It is important that the wider academy 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, Individual Schools will have an annual programme of training which is suitable to the audience. This will be mostly based around the CEOP ThinkuKnow (http://www.thinkuknow.co.uk) resources.

E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the academy, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

Staff Training - It is the responsibility of the Headteacher and the Governing Body to ensure that E-Safety training for staff is regularly planned, up to date and appropriate.

Prevent duty
The School is fully committed to safeguarding and promoting the welfare of all its pupils. Every member of staff recognises that safeguarding against radicalisation and extremism is no different to safeguarding against any other vulnerability in today's society.

- We protect children from the risk of radicalisation, for example by using filters on the internet to make sure they can't access extremist and terrorist material, or by vetting visitors who come into school to work with pupils.
- Our Safeguarding, Prevent Duty and eSafety policies set out our beliefs, strategies and procedures to protect vulnerable individuals from being radicalised or exposed to extremist views, by identifying who they are and promptly providing them with support.

Guidance for Staff (Guidance for safer working practice for those working with children and young people in education settings - October 2015)

Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used. Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.)

Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and this means that adults should:

- not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work
- not give out their personal details
- use only equipment and Internet services provided by the school or setting
- follow their school / setting's Acceptable Use policy
- ensure that their use of technologies could not bring their employer into disrepute 12 transparent and avoid any communication which could be interpreted as 'grooming behaviour'

Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable.

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 keep your computer in a place where everyone can use it, go online with your child so you can see what they are doing on the internet.
- 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 web sites, 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.

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 *(it may be easier and tidier to have a separate single sheet that all staff sign).*

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 in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff members 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 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 - 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 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 Mouchel Helpdesk 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 pupils.

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – Pupils

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the academy 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 :

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:**

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 - pupils	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Pupil laptops	Pupils 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 pupil 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 pupil accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the pupil.
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 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) :**