# Hope Corner School

## e-Safety Policy

# Table of Contents

## Policy Statement

This policy has been developed within the guidance found in "Keeping Children Safe in Education 2019" Annex C (online Safety) and paragraphs 84-87 (opportunities to teach safeguarding).

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

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

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

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

**Wider school community** – students, all staff, governing body, parents.

Safeguarding is a serious matter at Hope Corner 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 foreseeable harm to the student or liability to the school.

This policy is available for anybody to read on the Hope Corner 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.

Headteacher Name: Maria Houghton
e-Safety officer: Matthew Finch
Chair of Governors: Mark Finch

Policy Date: November 2020
Next Review Date: October 2021

## Policy Governance (Roles & Responsibilities)

### Governing Body

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

- Review this policy at least annually and in response to any 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.

- Appoint one governor to have overall responsibility for the governance of e-safety at the school who will:

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

### Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for 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. students, all staff, senior leadership team and governing body, parents.
- The designated e-Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All e-safety incidents are dealt with promptly and appropriately.

### e-Safety Officer

The day-to-day duty of e-Safety Officer is devolved to Matthew Finch

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all 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 e-safety incidents logged on Schoolpod; 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.
- Meet regularly with the e-safety governor to review the policy document.

**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.
    - 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. Passwords will be updated termly. Passwords for staff will be a minimum of 8 characters. A log will be kept of when passwords are updated.

**All Staff**

Staff are to ensure that:

- They understand all details within this policy. 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.
- They understand how to report an e-safety incident.

**All Students**

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

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

**Parents and Carers**

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

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

**e-Safety Group**

Each year we aim to establish an e-Safety group from volunteer students, the e-Safety Officer, responsible Governor and others as required. The e-Safety Group will meet on a termly basis.

The e-safety Group is responsible:

- to advise on changes to the e-safety policy.
- to establish the effectiveness (or not) of e-safety training and awareness in the school.
- to recommend further initiatives for e-safety training and awareness at the school.

## Technology

Hope Corner 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** – we use child safe filtering that prevents unauthorised access to illegal websites. Child safe are IWF members and block access to illegal Child Abuse Images and Content (CAIC). 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. Evidence of IWF membership and current internet filtering settings can be found in appendix 4.

**Email Filtering** – the school uses Zoho mail as our email host. The service automatically filters emails that do not pass DKIM and SPF authentication. Once an email is received it is also scared for viruses. AVG antivirus software also scans emails received against up to date virus definitions if staff have their email linked to an email client on their computer.

**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. All data stored in cloud services must be encrypted before being uploaded using Boxcryptor, a zero knowledge encryption software. Email is provided through Zoho Mail. This service encrypts data when at rest and uses SSL when messages are in transit.
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 local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.

**Passwords** – all staff and students will be unable to access computers without a unique username and password. Staff and student 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. Tablet computers are not password protected and so are only used when monitored by staff and are placed in locked cupboard when not in use. These tablets are not used for the storage of personal data.

**Anti-Virus** – All capable devices will have 'AVG' anti-virus software installed. 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 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 the 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. Similarly use of personal email addresses for work purposes is not permitted.

**Photos and videos** – When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

All parents must sign a photo/video release slip (as part of the yearly general parental consent) at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance. Students / pupils must not take, use, share, publish or distribute images of others without their permission. Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow the guidance, contained within this policy, concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

**Social Networking** – there are many social networking services available; Hope Corner 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 Hope Corner 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 communication tool to connect with other professional organisations and share one-way communications with the school community.
- Facebook – 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" or "friended" on these services and as such no two-way communication will take place.

Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts. Digital communications by staff must be professional and respectful at all times and in accordance with this policy.

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

- Permission slips (gathered as part of general annual parental permission) 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).

- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

**Remote Learning Tools** - During the coronavirus pandemic it has become essential to utilise a members area of the school website, zoom, and other tools that facilitate our remote learning offer. The school community must adhere to the guidance set by the school to use these appropriately and safely. The guidance is found in full in appendix 5 of this policy.

**Direct contact with students -** It is inappropriate for staff to use the personal contact details of students to contact them directly in any way. Home contact should only be made through parents and carers or if appropriate through remote learning tools as outlined in appendix 5.

In exceptional circumstances should there be a need for direct contact with a student; the reasoning, circumstances and process of doing this must be approved by the Designated Safeguarding Lead and head teacher. Parental consent must be sought to obtain the student's details. Contact should be made by the school text system, Teachers2Parents and copied to the parent. If a phone call is made, two staff members must be on the call. All contacts made in this way must then be logged as contacts on Schoolpod.

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

**Incidents** - Any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Headteacher. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an e-Safety cause for concern on SchoolPod, which are automatically flagged to the DSL and Head Teacher by the system. The e-Safety officer will work alongside the safeguarding officer to ensure the necessary actions are taken in accordance with the School's safeguarding policy. All incidents must follow the guidance in Hope Corner School's safeguarding policy, which all staff must be familiar with. The safeguarding policy follows the guidance found in "Working together to safeguard Children 2019".

## Training and Curriculum

**Online safety education in the school community -** 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, Hope Corner School will have an annual programme of training which is suitable for the audience. As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

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.

The e-Safety Training Programme can be found in this policy.

The school will support parents in e-safety at home by sharing relevant information about emerging technologies, key issues and equipping them with key skills

**In the curriculum -** 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 student's learning. e-Safety is embedded into the curriculum in various areas, such as key parts of the ICT functional skills courses, work in personal development lessons such as the DEAL course and as part of themed e-Safety days.

The school will utilise the Common Sense Education Digital Citizenship curriculum to support the developing of e-Safety awareness throughout our curriculum. This outlines 6 key categories within e-Safety. The school will focus on one of these key categories each half term and also cover the full range where appropriate.

The curriculum outline can be viewed here commonsense.org/education/system/files/digital_citizenship_curriculum_overview_2020_0.pdf?x=1

We will also use recourses from the SWGfL digital literacy curriculum to expand learning further. These can be found here http://www.digital-literacy.org.uk/Curriculum-Overview.aspx

**Radicalisation and Extremism** - our school ensures pupils are safe from terrorist and extremist material when accessing the internet in school, this includes establishing appropriate levels of filtering. If a concern arises students will know who to go to and adults should inform the Designated Officer for e-safety safeguarding who will act according to the Safeguarding Policy and the guidance outlined in the Prevent and Channel Duty Guidance. The digital citizenship curriculum will ensure are equipped and supported to remain safe online. Staff have taken part in Prevent training.

**Appendix 1: Acceptable Use Agreements**

# Staff Acceptable Use Agreement

*All staff must read this agreement in conjunction with the e-Safety Policy, the Information Security Policy and the Schools Information Security guidance. Once you have read all of these, please check them off below and then read and sign the agreement.*

I have read, understood and agree to the following:

☐ e-Safety Policy including appendix 5: Using Remote Learning Tools Safely

☐ Information Security Policy

☐ Schools Information Security Guidance (from Halton Council 9/18)

**Note: All Internet and email activity is subject to monitoring**

**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 report completed on SchoolPod.

**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. This must not happen even once students leave Hope Corner, whilst they are school age.

**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. Emails sent relating to the school must include a signature that follows the format provided in the e-safety documents file.

**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. Your computer must be set to require a password after the shortest inactivity time your computer allows.

**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. No one other than staff are permitted to access profiles containing school data on computers. School files are only permitted to be accessed through computers set up with Boxcryptor installed and set up.

**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.

*(Continued on reverse of page)*

**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 IT support as soon as it is practical to do so, along with the name of the virus (if known) and actions taken. AVG must be installed and running on any computer accessing school data.

**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.

**Copyright** – I will ensure that I have permission to use the original work of others in my own work. Where work is protected by copyright, I will not download or distribute copies (including music and videos).

**Communication outside school** - I will only contact families outside of school using the systems and steps outlined in the eSafety policy and remote learning tools guidance. I will never have direct 1-to-1 contact with students, unless there are exceptional circumstances approved by the head teacher, and I will follow the eSafety policy in these circumstances.

Name: _____

Signed: _____

Date: _____

# Student Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

# Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

- I will only use social media sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not try to download copies (including music and videos)

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school

network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.**

# Student Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, website etc.

Name of Student: _____

Signed: _____

Date: _____

Parent / Carer Countersignature_____

# Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form attached to show their support of the school in this important aspect of the school's work.

## Parent / Carer Permission Form

Parent / Carers Name: _____

Student Name: _____

As the parent / carer of the above students, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Signed: _____

Date: _____

## Appendix 2: Common Sense Eduction Digital Citizenship Curriculum Categories

# Cross-Curricular Framework

MEDIA BALANCE & WELL-BEING

We find balance in our digital lives.

**How can I make screen time meaningful?**
Learners go beyond "screen time" to explore the impact that their digital lives can have on their well-being and their relationships with others, while learning strategies for balancing media in their everyday lives.

PRIVACY & SECURITY

We care about everyone's privacy.

**How can I keep private data safe and secure?**
Learners find out how to protect personal information and gain a deeper understanding of their data privacy rights, so they can advocate for themselves and others.


DIGITAL FOOTPRINT & IDENTITY

We define who we are.

**How can I be responsible with my online identity?**
Learners consider the benefits and risks of online sharing and explore how their digital personae affect their sense of self, their reputations and their relationships.

RELATIONSHIPS & COMMUNICATION

We know the power of words & actions.

**How can I build positive relationships?**
Learners reflect on how to effectively communicate online and build positive relationships, avoid risky online talk, and understand why certain topics and conversations can best lend themselves to certain mediums.

CYBERBULLYING, DIGITAL DRAMA & HATE SPEECH

We are kind & courageous.

**How can I be kind and respectful?**
Learners take on these tough topics and play the active role of an upstander to build positive, supportive online communities and combat online cruelty.

NEWS & MEDIA LITERACY

We are critical thinkers & creators.

**How can I think critically about what I see and create?**
Learners will identify credible and trustful information sources and reflect on their responsibilities as thoughtful media creators and consumers.

"If all children could become good digital citizens then we would have a much happier, safer and mentally healthier human population. Common Sense Education recognises and addresses that hope by delivering highly thoughtful, engaging and relevant lessons on online safety."

– Dan Ferry, Teacher, Islington School, UK

***Prepare your learners to be digital learners, leaders and citizens.***

Get started at **commonsense.org/uk/digital-citizenship**

For more information contact **Jenna Khanna** at **jkhanna@commonsense.org**

common sense education®

## Appendix 3: e-Safety Training Programme

### Internal Training

Over the course of the year a different e-Safety curriculum category will be focused on each half term. To support this the e-Safety officer will carry out internal training with teaching staff, with a focus on the relevant category, before the start of each half term. This time will also be used to generate ideas for how this can be embedded throughout the school curriculum. Further time will be dedicated to refreshing staff about e-Safety policy and procedures, and raising awareness of emerging technologies and key e-Safety issues. The plan for this training is as follows:

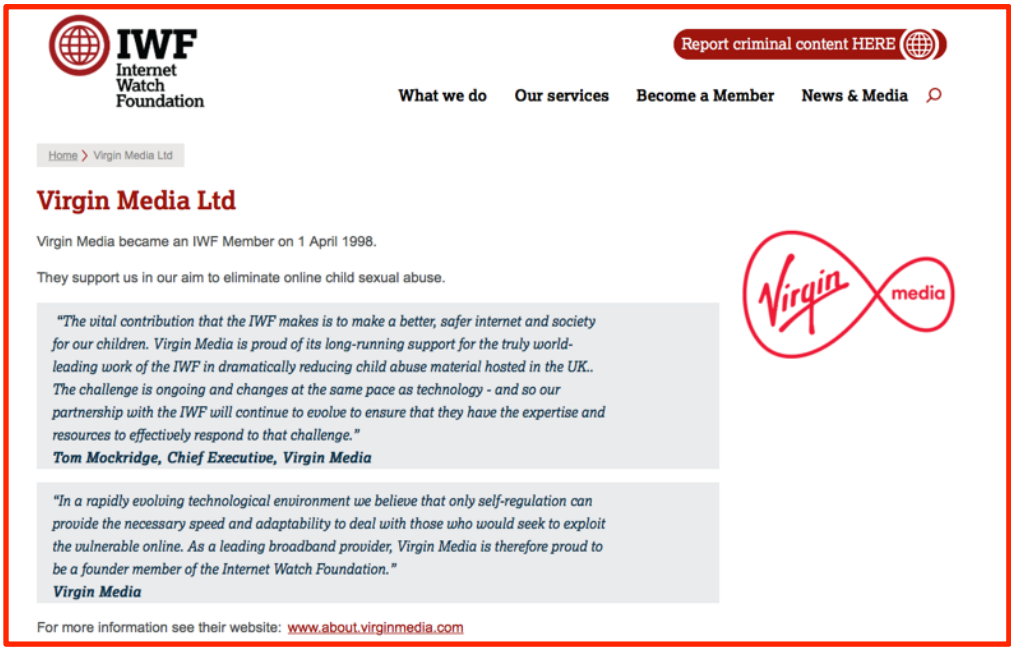
| Week Commencing | Key focus |
|---|---|
| 18th November 2020 | What is online identity and why does it matter? |
| 13th January 2021 | Balancing social media with our everyday lives |
| 3rd March 2021 | Helping students become critical thinkers when they consume online information. |
| 28th April 2021 | Curriculum Updates / Building positive online relationships. |
| 30th June | Equipping students to understand and utilise their online privacy rights. |
| To be completed as part of school inset day | How can our students help build positive communities online? |

The e-Safety officer will also keep staff up to date with relevant materials (e.g. websites, articles) in e-Safety. Key e-Safety items from the Halton Schools Weekly Update and the Halton Safeguarding Network termly update meetings will also be shared.

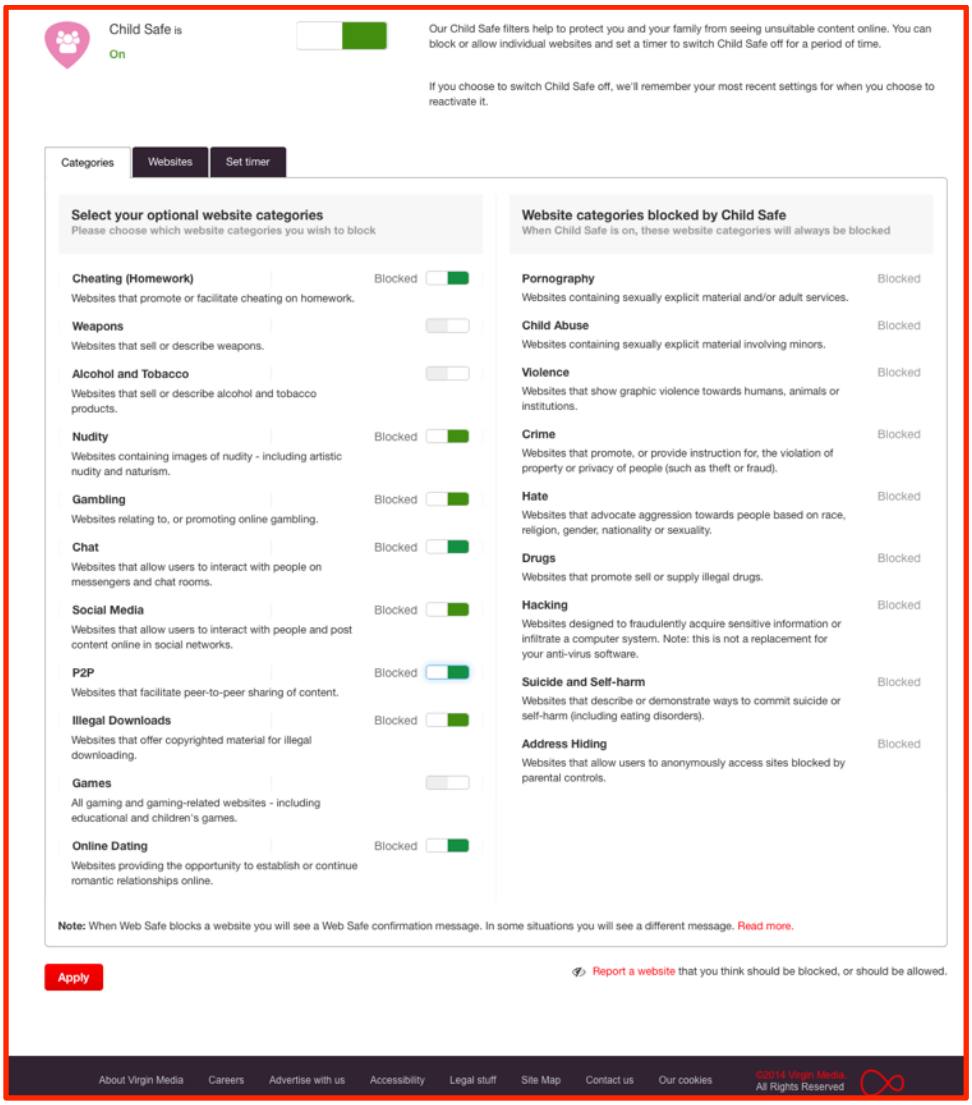
### External Training

The e-Safety officer will undertake a minimum of 20 hours of e-Safety CPD throughout the academic year. This may be attending events, reading current news, updating themselves on new technologies, software, apps or websites, or networking. Relevant information will be shared with the e-Safety group and with staff in order to implement necessary changes in the school.

## Appendix 4 - ISP IWF and Filtering Evidence




Left: IWF Virgin media membership




Left: ISP level content filtering settings

# Appendix 5: Using Remote Learning Tools

This document will outline the remote learning tools offered by Hope Corner School and detail how staff are expected to utilise these in a safe way. It is important that staff only communicate with students and parents as explained in this policy to maintain their own safety and that of our students.

Should any staff member, parent or student misuse these tools, the incident will be investigated and potential appropriate disciplinary action will be taken by the e-safety officer and head teacher.

All of our tools are under ongoing review and may change should they not be utilised or we deem them inappropriate for any reason.

Staff should adhere to the school E-Safety Policy and Staff Code of Conduct at all times.

**Online remote learning tool** - This is a digital tool that allows communication between home and school to enable learning through various methods, such as video chat, file sharing and more.

**Recording contacts made with teachers and students -** A contact should be recorded on schoolpod for any communication made through our online learning tools. Details will be outlined in each section below.

## Online remote learning tool descriptions

**Dropbox -** Online document storage and backup.

**hopecornerschool.co.uk member pages -** Area of our school website that students and staff need log in details to access.

**Zoom -** Group / conference online video and audio calling and screensharing.

**teachers2parents -** texting service that allows the school to text parents from a central online database, recording all communication that takes place.

## Using each tool safely and effectively

### 1. hopecornerschool.co.uk member pages

The school website contains two sections that staff or students must have log in details for an approved account to be able to access. These will be set up for students using parent's email address so parents are able to be more aware of communication taking place.

**Classrooms** - These are social pages with the idea of separating groups out into classroom spaces with each teacher. They work similar to a social media group where class members can post messaging or share videos/pictures.
The general use of these will be that teachers share their videos, link to other websites, videos and resources with ideas for tasks and activities students can carry out at home. Students and staff can leave comments on posts to share their thoughts/progress etc.

It is important that staff keep posts and discussion focused on topics centred around school, keeping healthy etc and must not be used to socialise. The e-safety officer will receive notifications whenever new content is posted in the classrooms and will flag and delete anything that is deemed inappropriate.

This feature will be under review and will be adapted or users will be removed if they are not using the tool appropriately.

**File Share -** This space is used for staff to upload documents, pictures etc they wish to share with students that will support them with their work. Students can view and download documents only, they cannot upload.

Staff must only use this space to share documents that relate to work students are completing and must not contain any personal information as all members can access all the documents in this area. Documents should be share as PDFs where possible to ensure they can be opened on any device.

As some students may find this area difficult to navigate, staff can copy specific document links and these can be pasted into the classrooms. Here students can click on the link and it will take them directly to the document teachers want students to access.

**Recording on Schoolpod -** Any contact made on our member pages that is more than discussing work would be recorded on Schoolpod in a contact. If anything a student shares or comments is inappropriate or out of character this should be recorded.

**2. teachers2parents**

Each staff member has a log in to this online based system. Group texts or texts to specific parents can be sent from here. Parents engage with this system well, so this is good to use if we need to communicate something to parents quickly. Staff can also check the system to see if parents have sent text responses to the school.

It is important that the 1st contact number is the only one used for texting parents of each student (this is the default setting on the system).

teachers2parents should be used to ensure parents have received emails we have sent to them and also used to send the meeting ID for zoom meetings. The system must not be used to send personal messages and parent phone numbers must not be copied or written down anywhere else.

It will also be used to follow up daily welfare calls if no contact can be made by phone

**Recording on Schoolpod -** All contacts to parents or received from parents are recorded onto schooled as a contact. The exception to this would be if a staff member is simply sending out a Zoom meeting ID or if a parent is flagging a technical issue.

**3. Dropbox** - As a general principal all of our data stored within dropbox is encrypted to a high level as outline in the e-safety policy. However we have temporarily added a folder for each student which is not encrypted. This will allow us to share documents with students by sharing a link to their child's folder.

We will not utilise this tool unless we need to start doing specific and tailored work for one student that needs to be kept separate to the rest of the documents we are sharing on our website 'file share' space.

Staff must be aware that personal information must still not be shared here and the folder is not encrypted.

**4. Zoom -** Online taught sessions on the remote learning timetable will be carried out using zoom. We will be doing this as group video and audio calls. Some calls will be made with individual students and others with a group of students. A specific process must be followed when making these calls which will be as follows:

Check zoom call timetable, only calls timetabled should be made. Nothing outside of these calls will be approved.
The lead staff member will set up a zoom meeting and generate the meeting ID & password.
**IMPORTANT:** Lead staff must switch screen sharing settings to 'host only' to prevent 'zoom bombing' risk before allowing anyone to join meeting.

1. Meeting ID & password should be shared with the other staff members scheduled to be in the lesson to allow them to join the meeting at least 5 minutes before the zoom call is scheduled to take place. Staff can briefly discuss what they will be covering the lesson. Staff members must never be in a call with students alone in order to safeguard the students and each other. If a staff member drops out for any reason and you are the only staff member remaining, you must immediately explain to the students you need to end the call and then proceed to do so.
2. Use teachers2parents to text the Meeting ID to parents to allow their child to join the zoom meeting.
3. Briefly discuss with students how they are generally. How they are using their time. Complete the lesson focusing on students gaining an understanding of the key concept and aim, or carry out any agreed interventions. Screens can be shared to support this, but staff must be extremely careful not to share personal information when doing this. The lesson should end when the teacher has assessed that the students are able to display an understanding of the key concept of the lesson. (How this looks may differ if this is one student joining a lesson when they are self-isolating)
4. Outline independent work that needs to be completed in the sessions of the timetable that have been identified.
5. Lead teacher ends meeting and one staff member records meeting on schoolpod.

**Recording on Schoolpod** - In most scenarios students engagement with lessons should continue to be recorded on Schoolpod as normal. However notes should also be added in the note of the green/amber/red slip for each student

# Risk Log

| No. | Activity | Risk | Likelihood | Impact | Score | Owner |
|---|---|---|---|---|---|---|
| 1. | Internet browsing | Access to inappropriate/illegal content - staff | 1 | 3 | 3 | e-Safety Officer |
| 1. | Internet browsing | Access to inappropriate/illegal content - students | 2 | 3 | 6 | e-Safety officer & teachers |
| 2. | Blogging | Inappropriate comments | 1 | 2 | 2 | Staff adding blog content |
| 2. | Blogging | Using copyright material | 2 | 1 | 2 | Staff adding blog content |
| 3 | Social Media | Uploading information/photos of students - staff | 1 | 3 | 3 | All Staff |
| 4 | Social Media | Issue developing through outside communication | 2 | 3 | 6 | All Staff |
| 5 | Twitter | Inappropriate communication with wider school community - staff | 1 | 2 | 2 | SLT |
| 6 | Tablet Computers | Access to inappropriate/illegal content - students | 1 | 3 | 3 | All staff |
| 6 | Tablet Computers | Taking and uploading photos of students | 2 | 2 | 4 | All Staff |
| 7 | Visitors' mobile devices | Taking and uploading photos of students | 2 | 2 | 4 | Staff welcoming visitors |
| 8 | Special phone permission | Accessing inappropriate content, contacting outside of the school, taking photos of other students | 2 | 3 | 6 | Staff monitoring student |
| 9 | Using online classrooms | Sharing inappropriate content, inappropriate contact between school community, online bullying | 2 | 3 | 6 | e-Safety Officer |
| | | | | | | |

**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**

# Risk Assessment 1

| Risk No. | Risk |
|---|---|
| 1 | Staff have access to school computers throughout the working day. This is also when students are present. There is therefore potential for them to try to access inappropriate or illegal content through the internet.<br><br>Students also have access to computers and tablet computers within the school with internet access. Similarly there is potential for students to purposefully or accidentally access inappropriate or illegal content. |
| Likelihood<br><br>1 - Staff<br>2 - Students | Based on thorough checks during recruitment, it is very unlikely any staff would purposely try to access illegal or inappropriate content.<br>Students are more likely to have a lack of understanding of content that is illegal or inappropriate and have had less training than staff in this area, so may access this without realising the negative impact it could have on them or others. |
| Impact<br><br>3 | The impact to the school reputation would be high. The staff members would have to be disciplined in accordance with the code of conduct. Depending upon the material accessed, they may not be permitted to work with students further, which impacts the quality of the school. If students access inappropriate material it could be upsetting to them, |
| Risk Assessment | MEDIUM (3 - Staff, 6 - Students) |
| Risk Owner/s | e-Safety Officer, Teachers |
| Mitigation | This risk should be actioned from both a technical and educational aspect:<br><br>Technical: Internet filtering applied at the router level of the internet to prevent access to illegal websites, or websites unsuitable for children. Log in details for each student on each computer will identify who has accessed each site.<br><br>Education: The e-Safety Policy training programme outlines the teaching and training that will take place for students and staff around the risks and consequences of accessing illegal sites of sites with inappropriate content. Staff, parents and students have also signed an acceptable use agreement clearly outlining that it is not acceptable to access these types of websites. |

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

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

# Risk Assessment 2

| Risk No. | Risk |
|---|---|
| 2 | The school has a blog as part of the school website. It posts news and event information onto it, and shares content about projects and achievements by students.<br><br>Whilst sharing this content with the public online, there is potential for inappropriate comments to be added to it and for copyrighted material, such as pictures or images to be used within the posts. |
| LIkelihood<br><br>1 - Inappropriate comments<br>2 - Copyright Material | It is unlikely that staff would use inappropriate comments within the blog posts as all staff are very aware of what is acceptable to write or share about relating to the school or students.<br><br>Accidental use of copyrighted videos, text or images may take place if staff are not fully aware or mindful of copyright. |
| Impact<br><br>2 - Inappropriate comments<br>1 - Copyright Material | If inappropriate comments are shared online this could reflect badly on the school, could trigger formal complaints from students, parents or public, or complaints to the DfE.<br>As we are a very small provision and we do not profit from posts on our blog the likely impact of accidentally using copyrighted martial is low. We would be asked to remove it if the copyright holder saw we had used it. |
| Risk Assessment | LOW (2 - Inappropriate content, 2 - Copyright material) |
| Risk Owner/s | Staff adding to the website blog |
| Mitigation | Regular refresher training on both appropriate conduct online and copyright use will be carried out with staff and students.<br><br>When adding a post to the blog 2 staff members will check the content before making the content live on the website to prevent inappropriate comments being made purposely or accidentally.<br><br>Only material created by the school, or labelled for reuse will be utilised within the school blog. Should a report be made about something breaching copyright the e-Safety policy will be followed. |

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

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

# Risk Assessment 3

| Risk No. | Risk |
|---|---|
| 3 | Staff uploading information or pictures of students they have access to, to social media websites. This may be purposely with intent or accidentally due to lack of awareness. |
| Likelihood<br>1 | Staff at the school are all DBS checked before they are allowed to work alongside students or have access to personal information from students. Photographs and personal information are not permitted to be taken or stored on personal devices. This means accidental upload is unlikely. |
| Impact<br>3 | The impact to individual students could be potentially very high if personal information or images are shared online. Due to the complex and vulnerable backgrounds some of out students come from having details shared online could cause inappropriate individuals finding students. Images shared online could damage self esteem if not shared in the correct way. |
| Risk Assessment | LOW (3) |
| Risk Owner/s | All satff |
| Mitigation | To reduce the risks of inappropriately sharing information online all staff must read our e-safety policy and sign the acceptable use agreement. They must also be DBS checked and read our safeguarding and data protection policies. Further internal training around safeguarding and e-safety will regularly take place to ensure understanding around using technology correctly as a staff member. This includes not using personal devices for pictures or sharing information online. |

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

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

# Risk Assessment 4

| Risk No. | Risk |
|---|---|
| 4 | Facebook and other social media allow communication with others. This means students and staff communicate with people outside the school community and issues can develop through this that have an impact on the school. |
| Likelihood<br>2 | It is likely that individuals will encounter issues with other people online, this may be minor or major issues. Younger students are more likely to encounter this as they may be less aware of safe online conduct. |
| Impact<br>3 | Arguments, speaking about inappropriate topics, grooming, radicalisation or more may be encountered. This can have a huge effect on staff or students within the school interns of their wellbeing, ability to work or learn, and can trigger procedures to protect them, which take up time and resources of the staff as a whole. |
| Risk Assessment | MEDIUM(6) |
| Risk Owner/s | All staff |
| Mitigation | On a technical level social media is block through the school ISP during school hours. This prevents individuals having inappropriate contact with negative influences during the school day in this method.<br><br>Educationally all staff are trained in the school's computer literacy programme so they are aware of dangers and can embed these skills into the curriculum to help students learn to be safe online. |

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

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

# Risk Assessment 5

| Risk No. | Risk |
|---|---|
| 5 | Inappropriate communication with the wider school community can occur through the school's twitter account. This may be contacting another organisation without permission, making a statement with an opinion not shared by the school leadership or more. |
| Likelihood<br>1 | It is very unlikely that inappropriate communication will take place through the school twitter account as only SLT have access to this account, who are very aware of the impact of messages displayed to the public can have upon the school. |
| Impact<br>2 | Reputation to the school could be damaged if twitter is used incorrectly or to share messages that reflect poorly upon the school. Links with organisations could also be damaged. |
| Risk Assessment | LOW(2) |
| Risk Owner/s | SLT with access to school twitter account |
| Mitigation | On a technical level social media is block through the school ISP during school hours. This prevents individuals having inappropriate contact with negative influences during the school day in this method.<br><br>Educationally all staff are trained in the school's computer literacy programme so they are aware of dangers and can embed these skills into the curriculum to help students learn to be safe online. |

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

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

# Risk Assessment 6

| Risk No. | Risk |
|---|---|
| 6 | Students are generally permitted to use the tablet computers within some lessons and at break times. They are connected to the internet. This can mean they have potential to access inappropriate or illegal content. They could also take pictures of other students and upload them online. |
| Likelihood<br>1 - Inappropriate content<br>2 - Photos | Students need to ask for permission from staff to have a tablet that can be used int he main area of the school. They could try to access inappropriate content although this would have to take place under the supervision of staff.<br>The camera on the tablets allow photography so they could take pictures and try to upload them online. |
| Impact<br>3 - Inappropriate content<br>2 - Photos | Accessing inappropriate content could cause harm to themselves or others. It could trigger safeguarding concerns or police contact, and could lead to exclusion.<br><br>Photos could be used for cyberbullying or make students feel their privacy has not been respected. This could cause trust issues or problems between students. |
| Risk Assessment | MEDIUM (3 - inappropriate content, 4 - photos) |
| Risk Owner/s | All Staff |
| Mitigation | Filtering takes place through the ISP to block inappropriate and illegal material and social media is blocked during school hours. Tablets are only permitted to be used under staff supervision. Staff lot a tablet out, monitor the student's use of the tablet and log the device back into the locked cupboard after use. Staff report misconduct with the divide to the E-Safety officer if it occurs.<br><br>Students all sign an acceptable use agreement outlining what is allowed to be accessed on school equipment and that they are not allowed to take pictures of other students on anything other than the school camera or without permission. If any of this is breached, permission to use the school equipment will be withdrawn.<br><br>Staff embed the computer literacy curriculum which develops the student's awareness of positive conduct online, and how to keep themselves safe and others, reducing the risk of these things occurring on the tablets. |

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

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

# Risk Assessment 7

| Risk No. | Risk |
|---|---|
| 7 | Students are generally permitted to use the tablet computers within some lessons and at break times. They are connected to the internet. This can mean they have potential to access inappropriate or illegal content. They could also take pictures of other students and upload them online. |
| Likelihood<br>2 | As visitors may not be aware of safeguarding issues within the education, or the vulnerability of our students they may take photographs and use them without understanding the impact. |
| Impact<br>2 | Photos uploaded online by visitors may be used in a way that reflects poorly on the school or upon the students. This is unlikely to be purposely done, but visitors may not understand what effect this does have. Students could also begin to feel unsafe, especially when visitors are present. |
| Risk Assessment | MEDIUM (4) |
| Risk Owner/s | Staff welcoming visitors to the school |
| Mitigation | All visitors must sign in when they arrive at the school reception. The door to the school is electrically locked so they cannot enter without being given permission. When they sign in it is expected that the staff member doing this will explain to the visitors that they are not allowed to used mobile phones or devices within the school and must seek permission to take any pictures. If this is breached it must be reported to SLT or the e-Safety officer. |

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

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

# Risk Assessment 8

| Risk No. | Risk |
|---|---|
| 8 | Specific student being permitted to use their smartphone during travel in the minibus to and from rock climbing (and possibly travelling to other educational visits). This is due to their anxiety during travel. This is closely monitored and handed in to staff before and after travel.<br><br>The student could use the phone inappropriately in terms of taking pictures of other students, accessing inappropriate content or contact people outside of the school. |
| Likelihood<br>2 | Student has a very limited time to use the phone and is monitored by staff. Although student could break their acceptable use agreement, student has been trustworthy to staff at this point, and is specifically using the phone for music. However photos, inappropriate communication or content could be access quickly. |
| Impact<br>3 | The impact to the school could be that other students question why they are not allowed to be using their phones, photos of students could be shared online by the student with their phone, or contact could be made outside of school that could cause issues in the school day.<br><br>(Having the phone enables student to travel calmly which was unlikely to happen without the phone.) |
| Risk Assessment | MEDIUM (6) |
| Risk Owner/s | Staff with student during the periods of time they have their phone. |
| Mitigation | Staff must consistently monitor student's use of the phone. It is only to be used during minibus journeys and not in any way that breaches the student acceptable use agreement. The phone must be only given to the student when leaving in the bus and collected from the student after the journey. If student seems to be using the phone inappropriately this risk will need to be immediately reviewed. |

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

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

# Risk Assessment 9

| Risk No. | Risk |
|---|---|
| 9 | Set up during the start of school closures during lockdown, we have an online classroom area on our website. Each student and staff member has an account to allow them to post work, videos, photos and comments in each of there teacher's classroom pages.<br><br>The use of this could create opportunity for staff and student to contact each other an inappropriate amount, individuals could share personal details, or inappropriate content. There could also be a chance that online bullying could take place. |
| Likelihood<br>2 | Although there is a chance for these risks to take place, staff are notified whenever any content is added to online classrooms so there is constant moderation. There are no forms of private contact so everything is visible to everyone. No one can access the classroom without an account that is given access to the classrooms by the school. |
| Impact<br>3 | Should harmful content be shared and then viewed by others before it is removed, this could cause forms of emotional and mental stress. Bullying could make students worry to return to school. Oversharing or inappropriate contact between staff and students could cause more serious consequences for individuals involved and the school reputation. |
| Risk Assessment | MEDIUM (6) |
| Risk Owner/s | eSafety officer |
| Mitigation | eSafety officer has app on their phone that notifies whenever any content is added to classrooms. This enables instant moderation and content can be removed quickly. Staff have been briefed in the safe use of the remote learning tools the school has. They have signed up to these rules, along with the acceptable use agreement, and understand the consequences should they not follow this. Any individual found to be using the classroom in an inappropriate way will have their account removed to prevent further access. Whenever anyone logs into the classroom space a message appears explaining how to report any concerns or worry individuals may have while they use the website. This directs them to an online form that allows them to share their concern with the safety officer. The eSafety officer with remove students from the system when they are no longer on the school role and with periodically check that parents still have access to their child's account so they can view their child's activity on the classrooms. |

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

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