



Online Safety Policy

Date issued: September 2022
Ratified by the Trust Board: December 2020
Review Date: September 2023

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

Policy Statement

For clarity, the online policy uses the following terms unless otherwise stated:

Users - refers to all staff, pupils, Trustees, 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 is an area that is constantly evolving and as such this policy will be monitored and reviewed every two years to ensure it remains fit for purpose.

The aim 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) 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 Online 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.

Roles & Responsibilities

In our Trust, all members of our community have a duty to behave respectfully both online and offline. Technology will be used for teaching and learning and prepare our pupils for life after school.

Trustees

Trustees are accountable for ensuring that our academies have effective policies and procedures in place; as such they will:

- Review this policy at every two year and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the academy, to ensure online incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint Trustees to have overall responsibility for the governance of online safety across the Trust:
 - Keep up to date with emerging risks and threats through technology use.
 - Receive regular updates from the Trust's Safeguarding Lead regarding training, identified risks and any incidents.

Headteacher

The Headteacher has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff (Designated Safeguarding Lead), as indicated below.

The Headteacher will ensure that:

- There is a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team, other stakeholders and parents.
- The designated Online Safety Officer has had appropriate training to undertake the day-to-day duties.
- All online incidents are dealt with promptly and appropriately, in accordance with related policies and procedures
- Suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of pupils being radicalised.
- Data management and information security is compliant with GDPR

Designated Safeguarding Lead/Online Safety Lead

The Designated Safeguarding Lead (DSL) should take the lead responsibility for safeguarding and child protection, including online safety, as per Keeping Children Safe in Education. However, the DSL may delegate certain online safety functions to other members of the Trust eg ICT Support Services.

The DSL will:

- Keep up to date with the latest risks to children whilst using technology, familiarising themselves with the latest research and available resources for school and home use.

- Ensure there is an effective approach to online safety which empowers the school to protect and educate in the use of technology and establish mechanisms to identify, intervene, and escalate any incident, where appropriate.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and Stakeholders on all online safety matters.
- Engage with parents and the school community regarding online safety matters at school and/or at home.
- Liaise with ICT technical support, or other agencies as required.
- Retain responsibility for online incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in the school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT technical support.
- Make themselves aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and Trust Safeguarding Lead 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 online 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 DSL and Headteacher.
- Passwords are applied correctly to all users regardless of age (NOTE: passwords for staff must be a minimum of 8 characters).

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 DSL or Headteacher.
- Any online safety incident is reported to the DSL (and an online safety incident report is made) or in their absence, to the Headteacher. If you are unsure, the matter is to be raised with the DSL or the Headteacher to make a decision.
- Part 1 and Annex C of Keeping Children Safe in Education is read and understood.
- All online material is checked fully before using either within the classroom or remotely
- The DSL is informed if this policy does not reflect practice, or if concerns are not acted upon promptly.

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.

Online 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. Our broad and balanced curriculum will give pupils an understanding of the benefits and opportunities, plus risk and dangers associated with the online world and know who to talk to if problems occur.

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 online 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.

Teaching & Learning

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

The online safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced regularly
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils will be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff will act as good role models in their use of digital technologies, the internet, and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- When pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- All video clips shown in class must be watched prior to being shown and checked for appropriate content.
- No content that is rated above the age of the pupils watching may be accessed or shown to children.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Special Educational Needs & Disability (SEND) & Vulnerable pupils

The Trust recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and Looked After Children (LAC). Relevant members of staff from within each individual academy, e.g. the SENDCO and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

Filtering and monitoring

Leaders have ensured that the Trust has age and ability appropriate filtering and monitoring in place, to limit pupil's exposure to online risks. The Trust is aware of the need to prevent "over blocking", as that may unreasonably restrict what pupils can be taught, with regards to online activities and safeguarding. Filtering and monitoring systems have been informed by a risk assessment, considering specific needs and circumstances and any changes to this approach will be risk assessed by staff with educational and technical experience and consent from the leadership team. Individual academy leaders will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate. As a Trust, we acknowledge that we cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is also essential. ICT technicians undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate. HCAT 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, Online 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.

All attempted breaches of our filtering systems are reported to the Designated Safeguarding Lead via the Smoothwall system. The Designated Safeguarding Lead will, where possible, ascertain further information and respond, record, and report accordingly. If the breach indicates that a child/young person may be at risk of significant harm, the DSL will respond immediately and may seek further advice and guidance from Children's Social Care and/or the police. Any incidents involving school staff will be reported to the Headteacher, and if necessary, the Local Authority Designated Officer (LADO) will be informed, along with Trust's Safeguarding Lead.

THE MARVELL COLLEGE

Mobile Technology - the college recognises that 3G, 4G or 5G 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 wireless mobile technologies 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.hcat.org.uk**.

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 not 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.

Use of digital and video images

Staff are allowed to take digital/video images to support educational aims but must ensure that these are transferred to a secure area on the school network/encrypted laptop immediately on return to school (if from an off-site visit) and before the camera is removed from site (if taken on-site). Staff are encouraged to use school equipment to take digital images and should not use own devices unless given prior permission by the head teacher. Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individual or the school into disrepute. Any images collected shall only be shared, used, published, or distributed in a way that is agreed by parents, e.g. staff will show compliance with the consent form signed by every parent in the school.

Images published on the school website will be selected carefully and will comply with good practice guidance, e.g. names shall not be published with images and all pictures will be within GDPR regulations.

The Data Protection Act 2018 does not apply to images of children taken purely for personal use by their parents/carers at an organised event. However, we do ask parents/cares to refrain from posting images on public forums, such as social media, so it does not adversely affect the safeguarding of pupils and staff.

Social networking

Our Trust is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents/carers and the wider school community. Should staff wish to use any form of social media, permission must first be sought from Senior Leader who will advise the Headteacher for a decision to be made. Any new social networking service will be risk assessed before use is permitted.

Before anything is uploaded, to the academy's social media site, the following **must** be applied:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupil using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy

Should it come to the academy's attention that there is a resource or image which has been inadvertently uploaded, and the school does not have copyright or permission to use, it will be removed within one working day.

CCTV

The school may use CCTV in some areas of school property as a security measure. Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff, and school together with its visitors. The Trust adheres to the Data Protection Act 2018, and guidance issued by the Information Commissioners Office (ICO).

Incidents

It is vital that all staff recognise that online safety is a part of safeguarding.

The Trust commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school).

All members of the school are encouraged to report issues swiftly to allow the Designated Safeguarding Lead to deal with them quickly and sensitively. It is imperative that all incidents are recorded on CPOMS. Staff could use the form (**Appendix A**) if they feel using this format would capture all the information better however, if this method is used, the form must still be scanned and uploaded onto CPOMS.

Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day.

However, if the risk is significant, the report should be reported, without delay, as evidence may need to be secured.

Any concern/allegation about staff misuse is always referred directly to the Headteacher unless the concern is about the Headteacher in which case the complaint is referred to the Chair of the Trust and the LADO (Local Authority's Designated Officer).

The school will actively seek support from other agencies as needed (i.e. the local authority -Children's Social Care, National Crime Agency, CEOP, Police, IWF). We will inform parents/carers of online safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (procedures are in place for child sexual imagery, sexting, up skirting etc).

Behaviour

Online communication can take many forms, whether it is by email, text, webcam, or instant chat. It is essential that all staff and learners are aware of the academy policies that refer to acceptable behaviours when communicating online.

- the academy will ensure that all users of technologies sign and adhere to the standard of behaviours set out in the Acceptable Use Policy
- the academy will not tolerate any abuse of its ICT network, infrastructure, or cloud-based systems, whether offline or online. All communications by staff and pupils should be always courteous and respectful.
- any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously.

Where conduct is found to be unacceptable, the academy will deal with the matter internally. Where conduct is illegal, the academy will report the matter to the police and other relevant external organisations as required/instructed.

Cyber Bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

There are different types of cyberbullying including:

- Text messages — that are threatening or cause discomfort — also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology).
- Picture/video-clips via mobile phone cameras — images sent to others to make the victim feel threatened or embarrassed.
- Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
- Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatrooms.
- Direct messaging (DM) — unpleasant messages sent while children conduct real-time conversations online using Snapchat, Instagram, Twitter, Facebook messenger etc.
- Bullying via websites and social networking sites — use of defamatory blogs, personal websites and online personal "own web space" sites.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimidated, 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 (often referred to as 'sexting', 'nudes'....');
- inappropriate sexual comments on social media.
- exploitation.
- coercion, or
- threats.

Any reports of online sexual harassment will be taken seriously, and the school's Child Protection procedures will be followed, which may require notifying the police and Children's Social Care.

PLEASE NOTE - Staff should **never** view any devices with alleged child sexual images, but **must** inform the DSL immediately, plus record accurately what has been reported.

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

Radicalisation Procedures and Monitoring

We will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in school and that suitable filtering is in place which considers the needs of pupils.

When concerns are noted by staff that a pupil may be at risk of radicalisation online then the Designated Safeguarding Lead will be informed immediately, and action will be taken in line with the Trust's Child Protection/Safeguarding Policy.

Searching devices

The Education Act 2006 allows staff to lawfully search electronic devices, without consent or parental permission, if they have **'good reason'** to suspect the device has been, or could be used, to cause harm, undermine the safe environment of the school and disrupt teaching, or be used to commit an offence.

If the member of staff conducting the search suspects, they may find an indecent image of a child (sometimes known as nude or semi-nude images), they should never intentionally view the image, and must never copy, print, share, store or save such images. When dealing with incident of this nature, the member of staff should confiscate the device, and refer the incident to the designated safeguarding lead (or deputy) as soon as possible.

In exceptional circumstances members of staff may dispose of the image or data if there is a good reason to do so. In determining whether there is a **'good reason' to erase** any data or files from the device, the member of staff should consider whether the material found may constitute evidence relating to a suspected offence. If the data or files are not suspected to be evidence in relation to an offence, a member of staff may delete the data or files if the continued existence of the data or file is likely to continue to cause harm to any person and the pupil and/or the parent refuses to delete the data or files themselves.

Further information please refer to the DfE guidance - Screening, Searching and Confiscation, July 2022

Staff Training

Staff are trained to fulfil their roles in online safety. Schools ensure that all staff are provided with regular training to improve their knowledge and expertise in the safe and appropriate use of the internet, mobile and digital technologies. All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential. Furthermore, staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with Trust policies (safeguarding, confidentiality, data protection etc.) and the wider professional and legal framework.

Remote Learning

In the event of a full or partial closure, the Trust is committed to ensuring pupils continue with their learning. Wherever possible, the Trust will continue to deliver live lessons using approved systems (eg Microsoft Teams).

Staff who interact remotely with pupil should continue to look out for signs that a child, or young person may be at risk. Any such concerns will be dealt with, as per the Trust's Child Protection policy and procedures, and where appropriate, referrals to Children's Social Care, and/or the Police will be made.

Guidance for safer working practice for those working with children and young people in education settings – February 2022

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, chatrooms, forums, blogs, websites, gaming sites, digital cameras, videos, webcams, and other handheld 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.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online 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 Online Safety incident, reported to the Online Safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the Online 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 Online 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.

Online Safety – like health and safety; online safety is the responsibility of everyone to everyone. As such you will promote positive online 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 :

Online Safety Incident Log

Name of person reporting incident:			
Date of report:			
Where did the incident take place:	Inside school?		Outside school?
Date of incident(s):			
Time of incident(s):			

Who was involved in the incident(s)?	Full names and/or contact details
Children/young person	
Staff member(s)	
Parent(s)/carer(s)	
Other, please specify	

Type of incident(s) (indicate as many as apply)			
Accessing age-inappropriate websites, apps, and social media		Accessing someone else's account without permission	
Forwarding/spreading chain messages or threatening material		Posting images without permission of all involved	
Online bullying or harassment (cyberbullying)		Posting material that will bring an individual or the school into disrepute	
Racist, sexist, homophobic, religious, or other hate material		Online gambling	
Sexting/Child abuse images		Deliberately bypassing security	
Grooming		Hacking or spreading viruses	
Accessing, sharing, or creating pornographic images and media		Accessing and/or sharing terrorist material	
Accessing, sharing, or creating violent images and media		Drug/bomb making material	
Creating an account in someone else's name to bring them into disrepute		Breaching copyright regulations	
Other breach of Acceptable Use Agreement			
Other, please specify			

Full description of the incident	What, when, where how?
Name all social media involved	Specify: Twitter, Facebook, Whatsapp, Snapchat, Instagram etc
Evidence of the incident	Specify any evidence provided but do not attach

Immediate action taken following the reported incident:	
Incident reported to Designated Safeguarding Lead /Headteacher	
Safeguarding advice sought, please specify	
Referral made to Children's Social Care	
Incident reported to police and/or CEOP	
Online safety policy to be reviewed/amended	
Parent(s)/carer(s) informed please specify	
Incident reported to social networking site	
Other actions e.g. warnings, sanctions, debrief and support	
Response in the wider community e.g. letters, newsletter item, assembly, curriculum delivery	

Summary of incident, investigation, and outcome (for monitoring purposes)	
--	--

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	Online 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	The inquisitive nature of children and young people is that they may actively seek out unsavory online content or come across such content accidentally. Therefore, the likelihood is assessed as 3.
3	
Impact	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.
3	
Risk Assessment	HIGH (9)
Risk Owner/s	Designated Safeguarding Lead IT Support
Mitigation	<p>This risk should be actioned from both a technical and educational aspect:</p> <p>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.</p> <p>Education: The Online 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 schoolwork only. The current school online safety education programme has already covered the safe and appropriate use of technology, pupils are up to date and aware of the risks.</p>

Approved / Not Approved (circle as appropriate)

Date:

Signed (Headteacher) :

Table of changes

Date	Change or inclusion
September 2022	Following the revised publication of KCSiE, and Screening, Searching and Confiscation, the following areas have been changed or added: <ul style="list-style-type: none">● Teaching and Learning● Filtering and monitoring● Incidents● Cyber bullying● Searching devices● Staff training