Harford Manor School

Foundations For Futures

Online Safety Policy

Date approved by Governors	4th December 2025
Last reviewed by	Colin Wheelhouse
Next review date	23rd September 2028
Person(s) responsible for review:	Colin Wheelhouse

Harford Manor School's Visions and Values **3**
Our Online Safety Aims: **4**
The 4 key categories of risk **4**
How do the 4Cs relate to online use and risk of harm? **5**
Content Risks 5
Contact Risks 5
Conduct Risks 6
Consumer Risks 6
2. Legislation and guidance **6**
Teaching online safety in schools 7
Roles and Responsibilities **7**
3.1 The governing board 7
All governors will: 8
3.2 The headteacher 8
3.3 The designated safeguarding lead (DSL) 8
3.4 The ICT manager 9
3.5 All staff and volunteers 10
3.6 Parents/carers 10
3.7 Visitors and members of the community 11
4.Education about Online Safety **11**
4.1 Online Safety Education for our Pupils 11
4.2 Online Safety Education for our Staff Community 12
4.3. Educating parents/carers about online safety 13
5.Cyberbullying **13**
Definition 13
Our approach to Cyberbullying 13
6.Using and Managing Access to Key Systems **13**
Using the Local Area Network (LAN) 14
Using the School Internet Connection 14
Using and Managing Social Media Outlets / Connections 14
Using and Managing Email Accounts 15
Staff using work devices / accessing servers outside of school 15
7. Responding to improper / unacceptable use of ICT Devices and Connections **16**
Staff 16
Pupils 16
8 Artificial intelligence* (AI) **16**
Links to other School Policies / Legislation / Guidance: 17
Policy Monitoring Arrangements 17
Appendix 1 18
Appendix 2: online safety incident report log 20

Harford Manor School's Visions and Values

Our School provides a safe, nurturing environment that promotes the five elements essential to positive well-being; being mindful and reflective, being active, giving back to others, being interested, learning new skills and connecting with the local and the wider community.

Our vision is to lay the foundations for life-long learning and positive well-being. We will develop and nurture life skills, independence, confidence and resilience to support each child in achieving their potential and to make a smooth transition to school and society itself.

Our vision is for each child to develop a curiosity of learning, discover their interests and grow in their love of learning.

Our Vision is a community where all children feel loved, respected and encouraged to develop to their fullest potential. We are committed to our families, providing support and encouragement.

We aim to offer a safe, happy place where everyone is known and valued, and where differing needs are acknowledged, accepted and met.

We aim to encourage each child to be independent and develop a sense of responsibility for themselves, and respect for others in the local and wider community.

Our school exists to provide a safe, developmentally, inclusive environment for all pupils.

Our Online Safety Aims:

This policy aims to:

- To set out the processes in place to help ensure the online safety of all users (pupils, staff, volunteers and governors) within the school setting
- To have an approach to online safety that allows the school to provide high quality access to the internet and deliver online learning safely
- To educate both pupils and our staff teams about how to use technology and the internet safely, at a level appropriate to each individual
- To outline procedures in place to report and support any related incidents when required
- Identify and support groups of pupils that are potentially at greater risk of harm online than others

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

The 4Cs classification also distinguishes between aggressive, sexual and value risks, as this is helpful in retaining a balanced view of the range of risks that children can encounter. We note that risks to the values that shape childhood and society are increasingly prominent.

In addition to the 4Cs, the new CO:RE classification recognises important cross-cutting risks, notably to children's privacy, health and fair treatment.

This is outlined in the table below:

Risks for Children in the Digital Environment			
Risk Categories	Conduct Risks	Contact Risks	Consumer Risks
Cross-cutting Risks	Privacy Risks (Interpersonal, Institutional & Commercial)		
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)		
	Risks on Health & Wellbeing		
Risk Manifestations	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Behaviour	Illegal Encounters	Financial Risks
	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

How do the 4Cs relate to online use and risk of harm?

Content Risks

Where a child is exposed to unwelcome and inappropriate content. This can include sexual, pornographic and violent images; some forms of advertising; racist, discriminatory or hate speech material; and websites advocating unhealthy or dangerous behaviours, such as self-harm, suicide and anorexia.

Contact Risks

Where a child participates in risky communication, such as with an adult seeking inappropriate contact or soliciting a child for sexual purposes, or with individuals attempting to radicalise a child or persuade him or her to take part in unhealthy or dangerous behaviours.

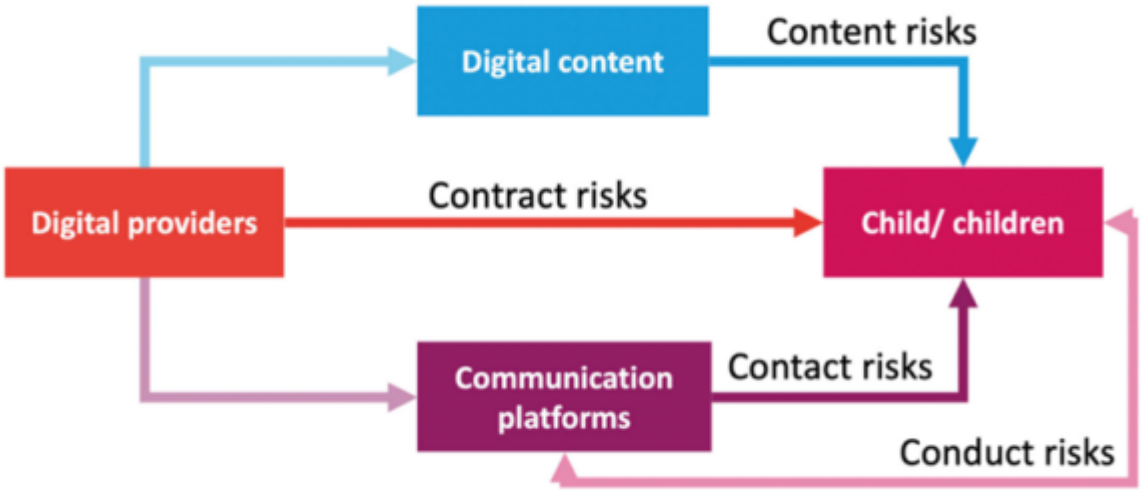
Conduct Risks

Where a child behaves in a way that contributes to risky content or contact. This may include children writing or creating hateful materials about other children, inciting racism or posting or distributing sexual images, including material they have produced themselves.

Consumer Risks

Consumer risks (also labelled 'commercial' or 'contract') arise when the child 'accepts' (including unintentionally, involuntarily or unknowingly) the Terms of Service (or Terms and Conditions) of a commercial provider of digital products or services. Such contractual arrangements can bind the child in ways that may be unfair or exploitative, or which pose security or safety or privacy risks of which they may be unaware or over which they have little control or means of escape. In short, contract risks arise when children use digital services as well as when they are impacted by digital transactions conducted by others in other ways.

Flow diagram of how the 4Cs impact children's online use:



2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

[Relationships and sex education –Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Academies, including free schools, if applicable, add/amend: This policy complies with our funding agreement and articles of association

Roles and Responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught (according to ability) how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;

Reviewing filtering and monitoring provisions at least annually;

Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;

Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Mark Lamb.

All governors will:

Ensure they have read and understand this policy

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures

Ensure that teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. This includes ensuring that teaching about online safety is appropriately adapted and differentiated for each individual pupil.

3.3 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and (deputy/deputies] are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks

Working with the ICT manager to make sure the appropriate systems and processes are in place

Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

Managing all online safety issues and incidents in line with the school's child protection policy

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the headteacher and/or governing board

Undertaking annual risk assessments that consider and reflect the risks children face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

Ensure that the all the school's ICT software systems are secure and protected against viruses / malware and that these systems are regularly updated

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are reported to SLT

Liaise directly with Norfolk ICT Shared services regarding all ICT and Internet usage / issues, including decisions on Wide Area Network (WAN) security

Take responsibility for the security of the schools Local Area Network (LAN) including set up and support for staff accessing the LAN (see below)

Ensure that all devices with internet capability have appropriate levels of security protection, filters and monitoring systems.

Regularly undertake reviews of the school's ICT systems, reporting any issues the Headteacher / Norfolk ICT Shared Services

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy

Implementing this policy consistently

Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)

Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the DSL and the ICT manager

Following the correct procedures by asking permission from SLT for a different level of filtering . (For example materials needed for teaching sex education) if they need to bypass the filtering and monitoring systems for educational purposes

Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

Notify a member of staff or the headteacher of any concerns or queries regarding this policy

Parents will be supported to raise awareness of online safety and best practice both at home and in school. Parents and carers are invited to contact the school (speaking to their child's class teacher in the first instance) to discuss any concerns they have regarding their child's online safety

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? – UK Safer Internet Centre

Hot topics – Childnet

Parent resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

4.Education about Online Safety

4.1 Online Safety Education for our Pupils

At Harford Manor School, our online safety education offer needs to be heavily adapted and differentiated to suit the complex and individualised needs of our pupils.

Any level of teaching regarding the safe use of ICT and online safety is tailored to individual students or small groups of pupils at the discretion of the class teacher. School leaders may also help to identify different groups for targeted intervention or areas of specific need across the school.

Online safety education may be taught as part of a structured ICT lesson with a whole class or smaller group of pupils, part of a targeted intervention for

individuals or small groups across multiple classes or individually as part of a pupils Personalised Learning Goals (PLGs) which are based on outcomes from their Education Health and Care Plans (EHCPs).

Teachers have access to a wide variety of lesson plans and resources provided through the schools National Online Safety membership that can be adapted to support online safety teaching across the school. These lessons offer a sequence of learning covering the following areas:

- Self-Image and Online Identify
- Online Relationships
- Online Reputation

- Online Bullying
- Managing Online Information
- Health, Wellbeing and Lifestyle
- Privacy and Security
- Copyright and Ownership

As part of these areas of development and teaching, key topics are covered based on individual pupil need and their level of understanding. A non-exhaustive list of these topics can be found below:

- Appropriate internet 'conduct' and identification of potential online risks including, hateful, harmful, illegal content and misinformation
- Pupil 'acceptable use' agreements / safety rules
- How use technology safely
- How to keep personal information secure online
- The use of ICT for communication purposes
- Safe and appropriate social media access
- Appropriate 'content' access and how to report inappropriate 'content'
- Appropriate 'contact' relationships / interactions and how to report inappropriate 'contact'
- Online 'stranger danger'
- How to identify and avoid 'consumer' risks online

4.2 Online Safety Education for our Staff Community

All new and existing staff members will receive regular training relating to online safety as part of our wider safeguarding training package.

Our online safety training will be determined and organised in accordance with the 'National Online Security' training platform / database to help ensure all staff are trained to the required level of competence and understanding in accordance with their role.

Key components of staff training relating to online safety are:

To raise awareness of the role online safety plays in many aspects of safeguarding and general pupil wellbeing

To highlight how pupils may be exposed to online dangers and abuse and how potential our students may abuse others online

To help staff identify signs and indicators of online abuse

To ensure staff know what do if they suspect online abuse or breaches of online safety policies have occurred

To support the development of clear and robust approaches to teaching online safety at appropriate levels to our students and to empower staff to deliver engaging and motivating lesson content in this key area

4.3. Educating parents/carers about online safety

At Harford Manor School we aim to support families and increase awareness of the potential risks online access poses at home both for their children and themselves. This will be facilitated in the following ways:

Providing access to relevant information and links regarding online safety through a dedicated page on our school website.

Sharing regular newsletters and information updates with parents

Providing access to 'Explainer Guides', 'Webinars' and online safety courses specifically designed for parents and carers through our National Online Safety membership

Our online safety policy will be made available to families through the school website

5.Cyberbullying

Definition

Cyberbullying can be defined as "the use of information communication technology, particularly mobile phones and the internet to deliberately hurt or upset someone" (DCSF). You people are being increasingly identified as both victims and perpetrators of cyberbullying incidents due to an increased exposure to ICT and the internet at younger ages.

Our approach to Cyberbullying

We encourage all our staff to adopt the approach of 'it could happen to anyone' when relating cyberbullying to our school and the pupils we support. All staff will receive training which refers to cyberbullying as part of the school's wider safeguarding training offer

To help prevent cyber-bullying, we will ensure that where appropriate, our pupils understand what cyberbullying involves and what to do if it is encountered at any level, including reporting incidents to school staff or trusted adults in the first instance. Any reported incidents of cyberbullying will be dealt with in accordance with the school's 'Bullying Policy'.

6.Using and Managing Access to Key Systems

Anyone accessing school ICT systems should do so in accordance with the school's ICT Code of Conduct (Appendix 1)

Using the Local Area Network (LAN)

All staff, including agency staff, School Governors and volunteers accessing the school LAN have a responsibility to ensure the LAN is accessed and used appropriately to support GDPR compliance. This includes:

- How to use technology safely and respectfully, keeping personal information private
- Logging off computers and ICT devices (such as iPads) when left unattended to protect sensitive information
- Storing devices safely and securely at all times
- Ensuring personal data is stored securely and used appropriately in school or remotely (using Safehouse software)
- Complying with copyright and intellectual property rights
- Ensuring that any pupils accessing the LAN are appropriately supervised and compliance with this policy is maintained

Using the School Internet Connection

All staff have a responsibility to use the school's internet connection, information systems and internet capable devices appropriately at all times They must also ensure that these are not used for any of the following activities. This includes when supervising pupils when accessing the internet.

- Conducting illegal activities
- Accessing or downloading pornographic material
- Gambling
- Soliciting for personal gain or profit
- Managing or providing a business or service
- Revealing or publicising proprietary or confidential information
- Representing personal opinions as opposed to those of the school
- Making or posting indecent remarks, images or proposals
- They must also comply with the guidelines set out below regarding the support and teaching of pupils about internet safety

Using and Managing Social Media Outlets / Connections

All staff, pupils, parents and carers need to be aware of the dangers social media networks potentially pose regarding both their own and others personal information and access to unmediated content.

- Norfolk ICT Shared Services will manage / control access to social media websites

- Staff should not access personal social media accounts using school servers or equipment
- Only official school social media accounts should be accessed using school servers by authorised staff members
- If staff use personal social media platforms then they should take appropriate measures to ensure do not bring the school into disrepute
- Staff should not publish any school related information / data or any private opinions regarding the school in the public domain
- Staff should not make connections with school pupils or their families via social media platforms

Using and Managing Email Accounts

The use of email is an essential means of communication to facilitate effective working on a day to day basis for many of our staff at Harford Manor School. Some pupils may also access emails as they explore the use of technology for communication purposes. However, it is important to follow the guidelines below to minimise risks regarding data protection and unwanted contact with third parties.

- Staff should only use pre-approved (@harfordmanor.school) email accounts for school related purposes / correspondence
- All contact between staff and pupils or families will take place using these approved school email addresses (@harfordmanor.school) and be monitored as appropriate
- Pupils accessing their own (set up by school) or class-based email accounts should be supervised by supporting adults at all times
- Pupils must not reveal any personal details about themselves to others or arrange to meet anyone using their emails
- Where possible, pupils must report any offensive or inappropriate email correspondence to their class teacher immediately
- Any email received by an unknown sender should be treated as suspicious and any attachments should remain unopened before reporting this to the ICT Technician

Staff using work devices / accessing servers outside of school

- All staff members will take appropriate steps to ensure their devices remain secure and access to school servers are not compromised by:
- Keeping the device password-protected using a strong password
- (at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters)
- Ensuring their hard drive is encrypted (using 'SafeHouse' or other approved software)
- Ensuring their device software (including anti-virus software) and other operating systems are regularly updated by the ICT Technician

- Ensuring that the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Contacting the ICT Manager immediately if they have any concerns regarding the security of their device / server access

Staff using personal mobile devices to access school accounts.

It is recognised that some staff may wish to be able to access systems such as school email accounts on a personal device. The school recognises that this is an individual's personal choice and does not mandate this. This potentially causes a Cybersecurity risk, in order to mitigate this risk

- to access school Google Workspace apps and accounts on a personal device staff must give consent to use the Google MDM policy on their device. This allows the school to remove any accounts and data relating to a school account in the event of loss, theft, damage or the end of employment. Staff must also inform the school at the soonest opportunity if a personal device with school accounts accessible from it is lost or stolen so that these accounts can be remotely wiped from the device.

7. Responding to improper / unacceptable use of ICT Devices and Connections

Staff

The headteacher / ICT Manager will monitor the use of the school's devices, information systems and internet access by staff. This includes the option/right to search the content stored on devices used within school, intercept staff email correspondence and delete any materials deemed inappropriate or where unauthorised use of the school's systems or data is believed to be occurring.

Any misuse of the school's ICT systems, included but not limited to those outlined above may result in disciplinary action in line with the school's disciplinary procedure or legal proceedings depending on the gravity of misuse deemed to have taken place.

All incidents will be recorded by the DSL or Headteacher in the on-line reporting log which will kept as and encrypted document on drive

Pupils

If a pupil is adjudged to misuse the school's ICT devices, systems or internet connection, then procedures set out in the school behaviour policy will be followed. Any action taken against the pupil(s) will depend on individual circumstances, the seriousness of the incident and the context in which it has occurred.

8 Artificial intelligence* (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini. Harford Manor School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. Harford Manor School will treat any use of AI to bully pupils very seriously, in line with our [anti-bullying/behaviour] policy.

Staff should be aware of the risks of using AI tools while they are still being developed and the school will carry out a risk assessment where new AI tools are being used and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff. Harford Manor School uses only Google Gemini for Education as its AI platform and any use of this artificial intelligence should be carried out in accordance with our AI usage policy.

Links to other School Policies / Legislation / Guidance:

This policy links to and informs the following school documents:

- The ICT Code of Conduct (Appendix 1)
- Website Policy
- The Mobile Phone and Smart Technology Policy
- Remote Learning Policy
- The Safeguarding Policy
- Bullying Policy

The information included in this policy is based on the Department for Education's (DfE) statutory safeguarding guidance:

- Keeping Children Safe in Education
- The Education Act 2010 / 11
- The SEND Code of Practice (2020)

Other guidance used to create this policy included:

- Livingstone, S., & Stoilova, M. (2021) The 4Cs: Classifying Online Risk to Children

- Becta ICT Advice (2005) E-Safety – Developing Whole School Policies to Support Effective Practice
- Norfolk County Council (No date) Model E-Safety Policy
- The Key for School Leaders

Policy Monitoring Arrangements

The Assistant Headteacher in charge of safeguarding (DSL) will have overall responsibility for monitoring and reviewing this policy supported by other key staff linked to ICT, such as the school ICT Technician and Website Co-Ordinator.

The policy should be reviewed on an annual basis and approved by the Governing Body and Headteacher.

Appendix 1

Harford Manor School's ICT Code of Conduct / User Agreement

This document is expected to apply to all staff members, including members of the Governing Body, school volunteers and any visitors accessing school ICT systems.

Harford Manor School acknowledges that the use of ICT and related technology such as emails and access to the internet are key components to successfully carrying out working roles within the school for a wide variety of purposes. However, to ensure the safety of our pupils, other ICT users, school data and to protect wider school systems, all ICT users must agree and sign this user agreement, acknowledging the statements below:

The term ICT refers to a wide variety of school systems, including PCs, laptops, tablets, cameras, mobile phones, email and internet access

This may include personal devices when used for school purposes

- I will not use personal ICT to record images / videos of pupils.
- I will only use school hardware for purposes authorised and permitted by the Headteacher in accordance with the school's online safety policy.
- I will only access to the school's internet / local area network (LAN) for purposes authorised by the Headteacher as outlined in the school's online safety policy.
- I understand that it is an offence to use the school ICT systems or equipment for any purpose not permitted by its owners.
- I understand that I am responsible to any activity carried out under my log in details on the school system.
- I will not browse, download, upload or distribute any material online or via school servers that may be considered offensive, illegal or discriminatory.
- I will not download or install any hardware or software without the express permission of the ICT Technician / Headteacher.
- I am aware that the school can monitor / server and internet access
- I will ensure GDPR compliance at all times and not disclose any personal information relating the school, its staff of pupils without the express consent of the Headteacher.
- I will ensure any information transferred either physically or electronically is done so securely to the best of my ability.
- I will only use approved school email accounts for school business
- I have a duty to complete school online safety training on an annual basis.

- I agree to be a good role model for pupils regarding my ICT access and will support appropriate online safety teaching in accordance with the school curriculum.
- I have access to the Whole School Online Safety Policy (via the school website) and should review this document for clarification regarding ICT use if required.
- I have read and understood the school's policy on the use of AI and how it can be used in my role at Harford Manor School.
- I will not jeopardise the safety or wellbeing of any pupil or colleague through my use of ICT.
- I will report any incidents or concern regarding the use of ICT within Harford Manor School to the Designated Safeguarding Lead (DSL - Cathie McLeod) or an Alternate DSL in her absence.
- I have a responsibility to seek clarification about any of the points made above with my line manager if required.
- I agree to follow this code of conduct when using school ICT (software and hardware) and network connections to ensure the safe use of ICT throughout Harford Manor School.

Name: _____ (print)

Role: _____

Signature: _____

Date: _____

Appendix 2: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident