2025

HURLEY PRIMARY SCHOOL

ONLINE SAFETY POLICY

ONLINE SAFETY POLICY

Date of publication: **September 2025** Review date: **September 2027**

Reviewed by:

Headteacher	**Matt Hardman, Headteacher**
Date:	**September 2025**
Online Safety Officer:	**Matt Hardman, Headteacher**

BACKGROUND AND RATIONALE

The impact of technology on our lives increases year on year and this is probably even more true for children. Technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live, behave and interact.

Although technology brings many opportunities, it also brings risks and potential dangers. This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where school have no control over the technical structures that we put in place to keep them safe at school) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

POLICY AND LEADERSHIP

This section begins with an outline of the **key people responsible** for developing our Online-safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain **how we maintain our policy** and then to outline **how we try to remain safe while using different aspects of ICT**

RESPONSIBILITIES: ONLINE-SAFETY COORDINATOR

Our online-safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to online-safety. The online-safety coordinator:

- takes day to day responsibility for online-safety issues and has a leading role in establishing and reviewing the school online-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online-safety incident
- provides training and advice for staff
- liaises with the Local Authority/ICTDS
- receives reports of online-safety incidents and creates a log of incidents to inform future online-safety developments
- meets with online-safety governor to discuss current issues and review incident logs
- reports to Headteacher
- receives appropriate training and support to fulfil their role effectively
- has responsibility passing on requests for blocking/un blocking to the ICT Helpdesk
- be responsible for the disposing of old IT equipment

RESPONSIBILITIES: GOVERNORS

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about online-safety incidents and monitoring reports. A member of the governing body has taken on the role of online-safety governor which involves:

- regular meetings with the Online-safety Co-ordinator with an agenda based on:
    - monitoring of online-safety incident logs
    - monitoring of filtering change control logs
    - reporting to relevant Governors committee / meeting

RESPONSIBILITIES: HEAD TEACHER

- The head teacher is responsible for ensuring the safety (including online-safety) of members of the school community, though the day to day responsibility is delegated to the Online-safety Co-ordinator
- The head teacher should be aware of the procedures to be followed in the event of a serious online-safety allegation being made against a member of staff.

RESPONSIBILITIES: CLASSROOM BASED STAFF

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online-safety matters and of the current school online-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Policy for staff
- they report any suspected misuse or problem to the Online-safety Co-ordinator
- digital communications with students (e.g. email/blogging) should be on a professional level and only carried out using official school systems (school portal/email)
- online-safety issues are embedded in the curriculum and other school activities

RESPONSIBILITIES: ICT TECHNICIANS (INTERNAL AND EXTERNAL)

The ICT Technicians (external) are responsible for ensuring that:

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are dealt with or reported to the ICT Development Service

POLICY SCOPE

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, and community users) who have access to and use school ICT systems, both on and off the school site.

Under the Education and Inspections Act 2006, headteachers have the authority to regulate pupil behaviour to a reasonable extent when pupils are off-site, including online behaviour. This includes incidents of cyberbullying, sexual harassment, or other online safety concerns that are linked to membership of the school community and that may pose a threat or cause harm to others, disrupt the orderly running of the school, or affect the school's reputation.

The school will address such incidents in line with this policy, the behaviour policy, the anti-bullying policy, and safeguarding procedures, involving the designated safeguarding lead where appropriate. Victims of online harm will be supported and reassured, and all incidents will be taken seriously regardless of when or where they occur.

Parents and carers will be informed of any significant incidents of inappropriate online behaviour that occur outside of school when these incidents are known to the school, ensuring a collaborative approach to pupil welfare and safety.

ACCEPTABLE USE POLICIES

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Staff (and volunteers if using school ICT)
- Pupils (EYFS + KS1 / KS2)

Acceptable use policies are revisited and re-signed annually at the start of each school year.

For children in EYFS and KS1 parents may sign on behalf of their children

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy

Parents sign a form which requesting permission for the use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish images of them on the school Facebook page.

Induction policies for all members of the school community include this guidance.

ILLEGAL OR INAPPROPRIATE ACTIVITIES AND RELATED SANCTIONS

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally, the following activities are also considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business
- Revealing or publicising confidential information (e.g. personal information, network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- On-line gambling
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

POSSIBLE PUPIL SANCTIONS

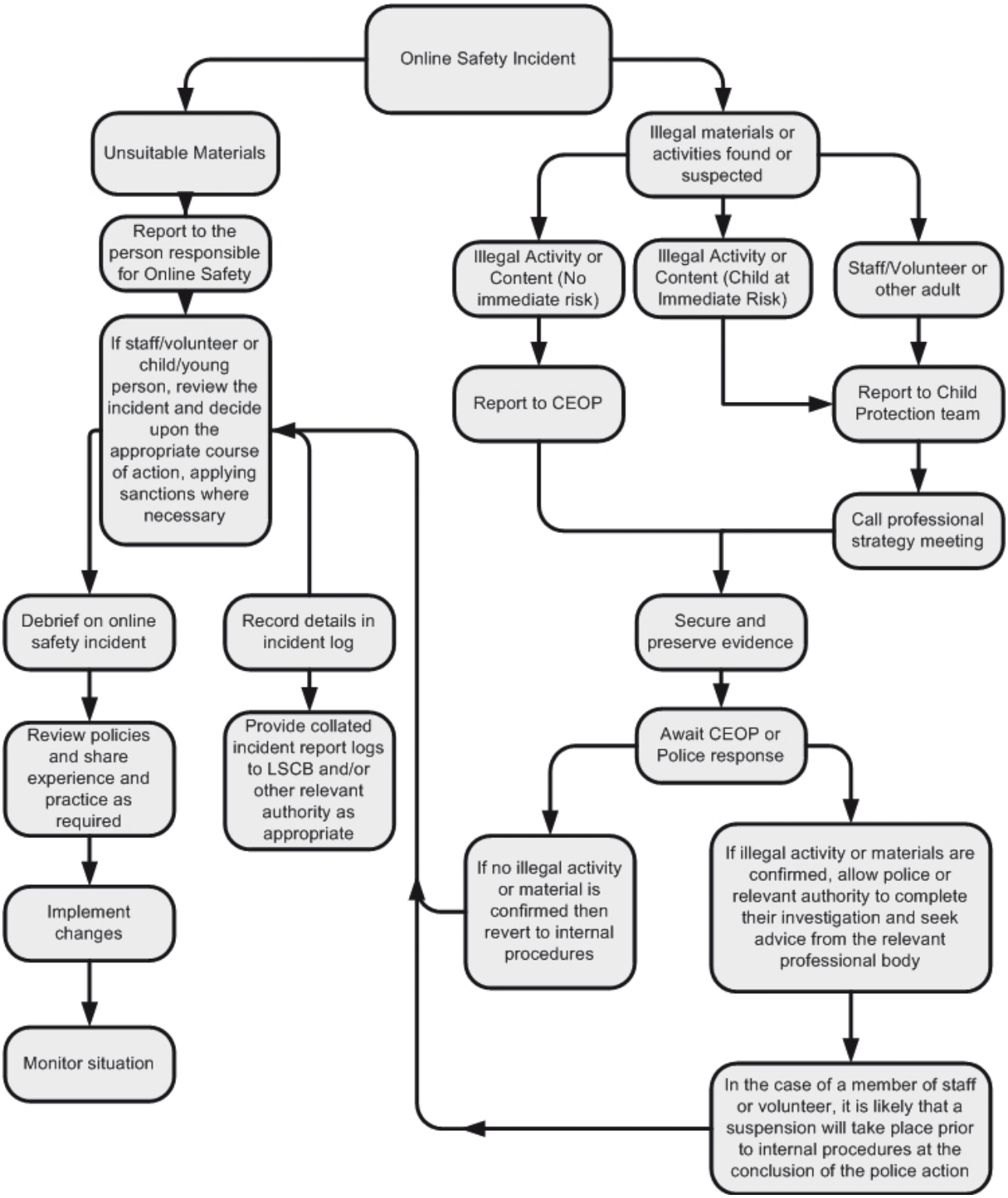
	Refer to class teacher	Refer to online-safety coordinator	Refer to head teacher	Refer to Police	Refer to online-safety coordinator for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓		✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓				✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓			✓			✓
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓				
Unauthorised downloading or uploading of files	✓				✓				
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓				
Attempting to access the school network, using another pupil's account	✓	✓	✓		✓		✓		
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓		✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓		✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓			✓		✓	
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓	✓	✓	✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓		✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✓	✓	✓		✓	✓	✓	✓	

STAFF SANCTIONS

	Refer to Online-safety coordinator	Refer to head teacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓	✓			✓	✓		
Unauthorised downloading or uploading of files	✓	✓			✓	✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓				✓		
Careless use of personal data eg holding or transferring data in an insecure manner	✓	✓						
Deliberate actions to breach data protection or network security rules	✓	✓			✓	✓	✓	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓	✓	✓			✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓	✓	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	✓	✓	✓			✓		
Actions which could compromise the staff member's professional standing	✓	✓				✓		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓				✓		
Using proxy sites or other means to subvert the school's filtering system	✓	✓			✓	✓	✓	
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓		✓	✓	✓	✓
Breaching copyright or licensing regulations	✓	✓				✓		
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓			✓	✓	✓

REPORTING OF ONLINE-SAFETY BREACHES

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:



AUDIT / MONITORING / REPORTING / REVIEW

The Online-safety coordinator will ensure that full records are kept on CPOMS of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the head teacher / and a governor on a termly basis.

USE OF HAND HELD TECHNOLOGY (PERSONAL PHONES AND HAND HELD DEVICES)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
    - Personal hand-held devices will be used in lesson time only in an emergency or extreme circumstances or to access Class Dojo
    - Members of staff are free to use these devices in school, outside teaching time.
- Pupils are not currently permitted to bring their personal hand-held devices into school. If children need a phone for some reason (e.g. they are staying at another child's house that night), the phone must be handed in to the school office at the start of the day and collected at the end of the day.

USE OF COMMUNICATION TECHNOLOGIES

Email

Access to email is provided for all users in school via Warwickshire Learning Platform – Welearn365.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access). This is particularly important in order that we meet new General Data Protection Regulation (GDPR) standards.
- Users need to be aware that email communications may be monitored
- Pupils have access to an individual email account for communication within school.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Users must immediately report, to their class teacher / online-safety coordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

- When using digital images, staff should inform and educate 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.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should be captured using school equipment; if a personal device is used, images should be deleted from the device after processing on Dojo.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission and must be educated as such.
- See also the following section for guidance on publication of photographs

Videoconferencing

- Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.
- Videoconferencing contact information should not be put on the school Website.
- Only web-based conferencing products that are authorised by the school are permitted for classroom use (Google Meet).
- Videoconferencing is always supervised by a teacher.
- Only key administrators have access to videoconferencing administration areas.
- Unique log on and password details for the educational videoconferencing services are only issued to members of staff (eg via Google Classroom)

Use of web-based publication tools

Our school uses the public facing website www.hurleyschool.co.uk and Facebook for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

School Portal

- Warwickshire ICTDS monitor the use of the learning platform by pupils regularly in all areas, but with particular regard to messaging and communication.
- Staff use is also monitored by Warwickshire ICTDS.
- User accounts and access rights can only be created by Warwickshire ICTDS.
- Pupils are advised on acceptable conduct and use when using the portal.
- Only members of the current pupil, staff and governor community will have access to the portal.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the **Teachers' Standards** as described by the DfE https://www.gov.uk/government/publications/teachers-standards. Teachers translate these standards appropriately for all matters relating to online-safety.

Any digital communication between staff and pupils or parents/carers (email, chat, portal etc) must be professional in tone and content.

- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

FILTERING

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Warwickshire's ICT Development Services, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **online-safety coordinator and the Warwickshire ICTDS** (with ultimate responsibility resting with the **head teacher and governors**). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

All users have a responsibility to report immediately to class teachers/online-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's online-safety curriculum as part of the PSHE and computing curricula.

Staff users will be made aware of the filtering systems through:

- signing the AUP (a part of their induction process)
- briefing in staff meetings, training days, memos etc. (from time to time and on-going).

Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through online-safety awareness sessions / newsletter etc.

Monitoring

- No filtering system can guarantee 100% protection against access to unsuitable sites. The school and Warwickshire ICTDS will therefore monitor the activities of users on the school network and on school equipment.

Audit / reporting

Filtering is predominantly managed by Warwickshire ICTDS and their filtering systems. If changes need to be made, this will be requested by a teacher/safety coordinator and the ICTDS will implement these. Logs of filtering incidents are made available to

- the online-safety governor
- the Warwickshire Safeguarding Children Board (WSCB) on request

This filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability

of the current provision.

ONLINE-SAFETY EDUCATION

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 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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

Online-safety education will be provided in the following ways:

- A planned online-safety programme is provided as part of computing and PHSE lessons and is regularly revisited – this will cover both the use of computers and new technologies in school and outside school
- Key online-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- 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.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

INFORMATION LITERACY

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as:
    - Checking the likely validity of the URL (web address) and AI interactions
    - Cross checking references (can they find the same information on other sites)
    - Checking the pedigree of the compilers / owners of the website
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require

THE CONTRIBUTION OF THE CHILDREN TO ONLINE-LEARNING STRATEGY

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning.

Pupils play a part in monitoring this policy.

STAFF TRAINING

It is essential that all staff receive online-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online-safety training as part of their induction programme, ensuring that they fully understand the school online-safety policy and acceptable use policies which are signed as part of their induction
- The Online-safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the WSCB and others.
- The Online-safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

GOVERNOR TRAINING

Governors should take part in online-safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in ICT, online-safety, health and safety or child protection.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or Learning and Achievement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The online-safety governor works closely with the online-safety coordinator and reports back to the full governing body.

PARENT AND CARER AWARENESS RAISING

Many parents and carers have only a limited understanding of online-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Parents information session – planned for new curriculum in Sept

WIDER SCHOOL COMMUNITY UNDERSTANDING

The school will offer family learning courses in computing, media literacy and online-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users who access school ICT systems / website / school portal as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

ACCEPTABLE USE POLICY AGREEMENT – PUPIL (KS1)

This is how we stay safe when we use computers:

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

I understand these computer rules and will do my best to keep them

My name:		Date
R - Signed (child):		
Y1 - Signed (child):		
Y2- Signed (child):		

ACCEPTABLE USE POLICY AGREEMENT – PUPIL (KS2)

I understand that while I am a member of Hurley School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will, wherever possible be supervised and monitored.
- I understand that my use of the internet will be monitored.
- I will keep my password safe and will not use anyone else's (even with their permission).
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others.
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not access anything illegal.
- I will not download anything that I do not have the right to use.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:		Date
Y3: Signed		
Y4: Signed		
Y5: Signed		
Y6: Signed		

Background

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed online-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (laptops, email, portal etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the online-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person (ICT coordinator or Headteacher).

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images, unless I have permission to do so.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the online-safety policy and then in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- 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).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the policy.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / Volunteer Name:	
Signed:	
Date:	