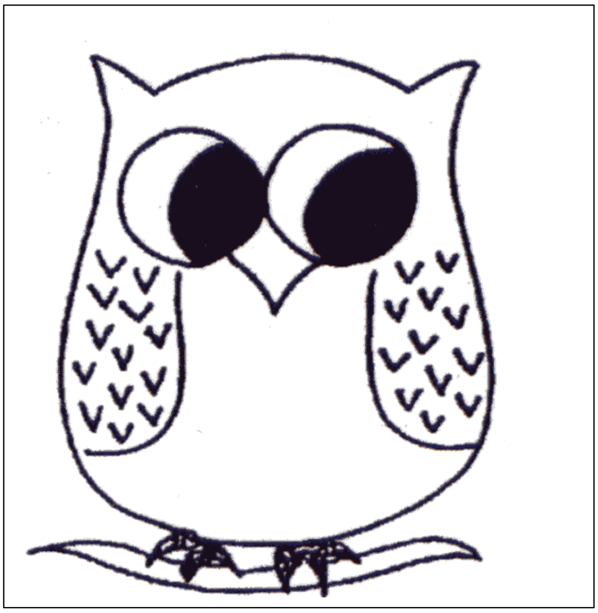
UPTON SNODSBURY C OF E FIRST SCHOOL



E SAFETY POLICY 2018

Upton Snodsbury C of E First School

E Safety Policy

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 we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about 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 gives an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school.

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

Responsibilities: the e-safety committee

Our school has an E-Safety Committee lead by our E-Safety/Safeguarding Coordinator, Teachers, the School Council members and our E-Safety Governor. It meets on an annual basis to:

- Review and monitor this E-Safety Policy
- Consider any issues relating to school filtering
- Discuss any e-safety issues that have arisen and how they should be dealt with

Issues that arise are referred to other school bodies as appropriate and, when necessary, to bodies outside the school such as the Worcestershire Safeguarding Children Board.

Responsibilities: e-safety

Our E-Safety Coordinator is the person responsible to the head teacher and governors for the day to day issues relating to e-safety. The E-Safety Coordinator:

- leads the E-Safety Committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technician
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reviews weekly the output from monitoring software and initiates action where necessary, if the e safety co-ordinator is absent from school the responsibility will be taken by the Head Teacher.
- meets regularly with E-Safety Governor to discuss current issues and review incident logs
- attends relevant meetings and committees of Governing Body
- reports regularly to Head Teacher
- receives appropriate training and support to fulfil their role effectively

Responsibilities: governors

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 e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor which involves:

- regular contact with the e-Safety Co-ordinator annually or as necessary with an agenda based on:

- monitoring of e-safety incident logs
- reporting to relevant Governors meeting

Responsibilities: Head Teacher

- The Head Teacher is responsible for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Co-ordinator
- The Head Teacher will be familiar with the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff, including non-teaching staff.

Responsibilities: classroom based staff

All staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: this duty is on the individual, not the organisation or the school
- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school's Acceptable Use Agreement for staff
- they report any suspected misuse or problem to the E-Safety Co-ordinator
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems
- they embed e-safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme

Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the e-safety technical requirements
- users may only access the school's networks through a properly enforced password protection policy
- shortcomings in the infrastructure are reported to the ICT Coordinator or Head Teacher so that appropriate action may be taken

Policy development, monitoring and review

This E-Safety Policy has been developed (from a template provided by Worcestershire School Improvement Service) by a working group made up of:

- E-Safety Coordinator
- Head teacher
- Teachers
- Support Staff
- Governors
- Pupils

Consultation with the whole school community has taken place through the following:

- Staff meeting
- School Council
- Governors meeting

Schedule for development / monitoring / review of this policy

This E-Safety Policy was approved by the governing body on:	Autumn 16
The implementation of this E-Safety Policy will be monitored by the:	e-safety coordinator
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive regular reports on the implementation of the E-Safety Policy generated by the E-Safety Coordinator (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding:	Termly at Full Governor Meetings
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	July 2017
Should serious e-safety incidents take place, the following external persons / agencies should be informed as appropriate:	Worcestershire Safeguarding Children Board e-safety representative (Martin Launan) Local Authority Designated Officer (Jane Finch) Worcestershire Senior Adviser for Safeguarding Children in Education (Sally Mills) West Mercia Police Diocese Representatives

Policy Scope

This policy applies to all members of the school community (including teaching staff, wider workforce, pupils, volunteers, parents / carers, visitors, community users, placement students) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Acceptable Use Agreements

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 Agreements are provided in this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff
- Parents / carers
- Community users, volunteers and student on placement of the school’s ICT system

Acceptable Use Agreements are introduced at parents’ induction meetings and signed by all children as they enter school (with parents signing on behalf of children below Year 2) Children resign on entering KS2.

All employees of the school 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 once when their child enters the school. The parents' policy also includes permission for 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 their work.

Community users will sign when they first request access to the school's ICT system.

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

Self Evaluation

Evaluation of e-safety is an on-going process and links to other self evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders, pupils, parent, teachers are taken into account as a part of this process.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies

ICT Policy	How ICT is used, managed, resourced and supported in our school.
E-Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The E-Safety Policy constitutes a part of the ICT policy.
School systems and Data Security Policy (IBS booklet)	How we categorise, store and transfer sensitive and personal data and protect school systems. This links strongly and overlaps with the e-safety policy.
ICT Progressions	Three key documents and associated resources directly relating to learning covering the ICT Curriculum

Other policies relating to e-safety

Anti-bullying	How your school strives to eliminate bullying – link to cyber bullying
PSHE	E-Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy
Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.
Use of images	WCC guidance to support the safe and appropriate use of images in schools and settings

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 equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council Broadband or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- On-line shopping
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)

If members of staff suspect that misuse might have taken place – whether or not it is evidently 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.

Pupil sanctions	**Refer to:**					**Inform:**	**Action:**		
	Class teacher	E-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security	Parents / carers	Remove of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓	✓	✓	✓	✓	✓	✓
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	✓						✓	✓	
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		Inform		Action		
	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering	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				✓	✓		
Careless use of personal data e.g. 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 students / 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	✓			✓			✓

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 (i.e. at the village hall to call school for help)
  - ✓ Members of staff are free to use these devices outside teaching time

- ✓ Taking photos on personal phones or other camera devices is not allowed

- Pupils are not currently permitted to bring their personal hand held devices into school
- There are devices available in school (I-pad, digital cameras) and these are used by children as considered appropriate by members of staff

Use of communication technologies

Email

Access to email is provided for all users in school via the Worcestershire Learning Gateway using their Global IDs. These official school email services may be regarded as safe and secure and are monitored using Policy Central

- Staff and pupils should use only the school email services to communicate with others when in school
- Users need to be aware that email communications may be monitored
- Pupils normally use only a class email account to communicate with people outside school and with the guidance of their class teacher
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email
- Staff may access personal email accounts on school systems for purposes such as emailing planning into school – rather than using a pen drive (that could carry viruses)
- Users must immediately report to their class teacher / e-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 they must not respond to any such email

Social networking (including chat, instant messaging, blogging etc.)

	Staff / adults				Pupils			
Use of social networking tools	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of non-educational chat rooms etc.				✓				✓
Use of non-educational instant messaging				✓				✓
Use of non-educational social networking sites				✓				✓
Use of non-educational blogs				✓				✓

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 only be captured using school equipment; the personal equipment of staff should not be used for such purposes, unless directed by the Head Teacher using the school memory card.
- 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.

Use of web-based publication tools

Website (and other public facing communications)

Our school uses the public facing website http://www.uptonsnodsburyfirstschool.org.uk only for sharing information with the community beyond our school. This includes, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website and only then when necessary .Full names are used on our newsletters without photographs attached
- Detailed calendars will not be 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 the 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 (agreements signed by parents)
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Learning Platform

Class Teachers monitor the use of the learning platform by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.

User accounts and access rights can only be created by the School Administrator / ICT co-ordinator

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers, governors, and staff community will have access to the learning platform.

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).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the learning platform may be suspended for the user.

d) The user will need to discuss the issues with the head teacher before reinstatement.

e) A pupil's parent/carer may be informed.

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access

Infrastructure

Password security

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school

Filtering

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 Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

Responsibilities for filtering

The day-to-day responsibility for the management of the school's filtering policy is held by the e-safety coordinator (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

All users have a responsibility to report immediately to e-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 have been filtered.

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 for filtering

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

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

- signing the Acceptable Use Agreement
- briefing in on-going staff meetings

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions

Monitoring for filtering

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment. Monitoring takes place as follows:

- Identified member of staff reviews the Policy Central (from Forensic Software) console captures weekly
- "False positives" are identified and deleted.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use so that the word can be allowed for the period of the topic being taught.

Audit / reporting for filtering

Filter change-control logs and incident logs are made available to:

- Head Teacher and the e-safety governor
- the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

Technical security

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document for more information.

Personal data security (and transfer)

This is dealt with in detail in **IBS School's System and Data Security advice**. Please see that document for more information.

Teachers discuss issues relating to data security and how it relates to staying safe in and out of school

Education

E-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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of ICT, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school
- We use the resources on the Worcestershire E-safety website as a source of e-safety education resources http://www.wes.networcs.net (e.g. Hector's World at KS1 and Cyber Café and SAFE social networking at KS2)
- Learning opportunities for e-safety are built into the Knowledge and Understanding sections of the Worcestershire Primary ICT Progressions where appropriate and are used by teachers to inform teaching plans.
- Key e-safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement 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, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging children to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

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)
    - ✓ Cross checking references (Can they find the same information on other sites?)
    - ✓ Checking the owners of the website
    - ✓ See lesson 5 of the Cyber Café Think U Know materials
    - ✓ Referring to other (including non-digital) sources
- Pupils will 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
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources

The contribution of the children to e-learning strategy

It is our general school policy to encourage 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.

Staff training

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

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-safety Co-ordinator will be CEOP trained
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE and the local authority
- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content
- The E-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 e-safety training / awareness sessions, with particular importance for those who are involved in ICT, E-Safety, Health and Safety or Child Protection. This may be offered in participation in school training / information sessions for staff or parents

The E-Safety Governor works closely with the E-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 e-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.

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

- Internet Safety presentation on school website with reference to the parents materials on the Worcestershire E-safety website http://www.wes.networcs.net and other useful websites
- Annual parents meetings to discuss the importance of e-safety, led by e-safety co-ordinator

Supporting resources and links

- http://www.ceop.gov.uk
- http://clickcleverclicksafe.direct.gov.uk/index.html
- http://www.thinkuknow.co.uk/default.aspx
- http://searchenginewatch.com/showPage.html?page=2156191
- http://www.wmnet.org.uk/21.cfm?zs=n
- http://www.saferinternet.org/ww/en/pub/insafe/index.htm
- http://www.wes.networcs.net

This policy was approved by Staff and Governors - Autumn 2018

Date of Review ………………………………………… **Signature** ……………………………………..………….

Date of Review ………………………………………… **Signature** ………………………………………………….

Date of Review ………………………………………… **Signature** ………………………………………………….

Upton Snodsbury C of E First School

Acceptable use policy agreement – pupil (FS & 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 if an adult says it is 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 turn off the monitor and 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:	
Parent's signature:	
Date:	

Upton Snodsbury C of E First School

Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Upton Snodsbury C of E First 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 be supervised and 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 try to 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.
- 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 of any type on the devices belonging to the school without permission.
- I will only use social networking, gaming and chat through the sites the school allows

KS2 Pupil Acceptable Use Agreement Form

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:	
Signed by child:	
Parent's signature:	
Date:	

Upton Snodsbury C of E First School

Acceptable Use Agreement – staff & volunteer

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 e-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.[through policy central.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person.

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.
- 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 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 ensure that my data is regularly backed up in accordance with relevant school policies (see **IBS Schools Systems and Data Security advice**).
- 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 transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted. [?]
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- 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 Agreement 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 to 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 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 police.

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:	

Upton Snodsbury C of E First School

Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- young people will be responsible users and stay safe while using ICT (especially the internet).
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect them to agree to be responsible users.

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

Child's name	
Parent's name	
Parent's signature:	
Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe and responsible use of ICT – both in and out of school.

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

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

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

Parent's signature:	
Date:	

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities and to provide valuable evidence of learning and assessment. Pupils and members of staff use the school's digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. The school will also ensure that when images are published, the young people cannot be identified by name.

As the parent / carer of the above pupil, I agree to the school taking and using digital images of my child. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at school events which include images of children, I will abide by these guidelines in my use of these images.

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's learning platform.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

The school's e-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Upton Snodsbury C of E First School

Acceptable use policy agreement – community user / student / governor

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

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

- I will not access, copy, remove or otherwise alter any other user's files or data, 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.

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 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 described above.
- 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, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the

event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community user / student / governor Name:	
Signed:	
Date:	