Reviewed Sept 2023
To be reviewed Sept 2027

Online Safety and Acceptable Use of the Internet Policy

2023

Technology is an important and essential part of the learning experience at Bewdley Primary School. We are committed to ensuring that our children leave with the skills and knowledge that will help them to thrive in our digital age. We have laptops in Key Stage 2 and iPads across the rest of the school planned to be used daily for research and educational apps. The teachers use the internet daily with the children. It is therefore also vital that we teach children how to use these valuable resources safely. This policy will appreciate that all children have access to smart phones, tablets and computers at home and within school. It promotes the use of these technologies whilst committing to keeping our children aware of, and safe from, the potential risks.

We will demonstrate that we have provided the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks. The Online policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people, their parents / carers and all staff to be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information (this is of particular concern under GDPR legislation);
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games, particularly age-inappropriate
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music, gaming or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.

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.

Our school's online safeguarding policy has been written from a template provided by Worcestershire School Improvement team which has itself been derived from that provided by the South West Grid for Learning.

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 technology. It also outlines the core responsibilities of all users of technology 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 technology.**

Responsibilities: Governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. A member of the governing body has taken on the role of online safety governor which involves:

- an annual review on online safety (as part of the Safeguarding Audit)
- monitoring of online safety incident logs
- reporting to relevant Governor's committee / meeting

Responsibilities: Headteacher/Online Safety Coordinator

- The Head Teacher is responsible for ensuring the safety (including online safety) of all members of the school community.
- The Head Teacher will be familiar with the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including non-teaching staff. (See Code of Conduct Policy and other relevant Local Authority HR / disciplinary procedures)
- The Head Teacher/senior leaders are responsible for ensuring the online safety leader and other relevant staff receive suitable CPD to enable them to carry out their roles and to train other colleagues as relevant.

Responsibilities: Online Safety Coordinator

Our online safety coordinator is the person responsible 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 school IT technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments

Responsibilities: Teaching and Support staff

Teaching and Support 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 online safety matters and of the current school Online safety policy and practices
- They have read and understood the 'Acceptable Use Policy' (AUP) and agreement.
- Digital communications with pupils are on a professional level and through the agreed areas e.g. Dojo.
- They report any suspected misuse or problem to the Online 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 online safety issues in the curriculum and other school activities, also acknowledging the planned online safety programme

- Pupils understand and follow the school rules regarding acceptable use of Computing.
- That they monitor computing activity in lessons, extra-curricular and extended school activities.
- Remind any members of staff who have an online safety concern, they should log it on CPOMS using factual information and speak to the DSL and IT Lead where appropriate.

Responsibilities: Designated Safeguarding Lead

The DSL should be trained in online safety issues and be made aware of the potential for serious child protection issues which may arise from:

- Sharing of personal data
- Access to illegal or inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying

Responsibilities: Technician

The Technician is responsible for ensuring that:

- The school's technology infrastructure and data are secure and not open to misuse or malicious attack
- The school meets the online safety technical requirements outlined in this policy (and any Relevant Local Authority Online Safety Policy and guidance)
- Users may only access the school's networks through a properly enforced password protection policy as outlined in the school's e-security policy
- Shortcomings in the infrastructure are reported to the Computing coordinator or Head Teacher so that appropriate action may be taken.

Policy Scope

This policy applies to **all members of the school community** (including teaching staff, wider workforce, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT 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 online 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 online safety behaviour that take place out of school.

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 IT 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 our technicians, Worcestershire County Council Broadband and / 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 gambling and non educational gaming
- 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 as indicated on the following pages.

Pupil sanctions

The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

	Refer to:					Inform:		Action:	
	Class teacher	Online safety coordinator	Refer to Head Teacher	Refer to Police	Refer to online safety coordinator for action re filtering	Parents / carers	Remove 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).	X	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X				X				
Unauthorised use of mobile phone / digital camera / other handheld device	X					X	X		
Unauthorised use of social networking / instant messaging / personal email	X	X			X	X		X	
Unauthorised downloading or uploading of files	X						X	X	
Allowing others to access school network by sharing username and passwords	X	X	X		X		X	X	
Attempting to access the school network, using another pupil's account	X				X		X		
Attempting to access or accessing the school network, using the account of a member of staff	X		X		X	X		X	
Corrupting or destroying the data of other users	X		X		X	X	X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X		X	X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X			X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X		X					X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X		X		X		X		

	Refer to:	Action:

Staff sanctions

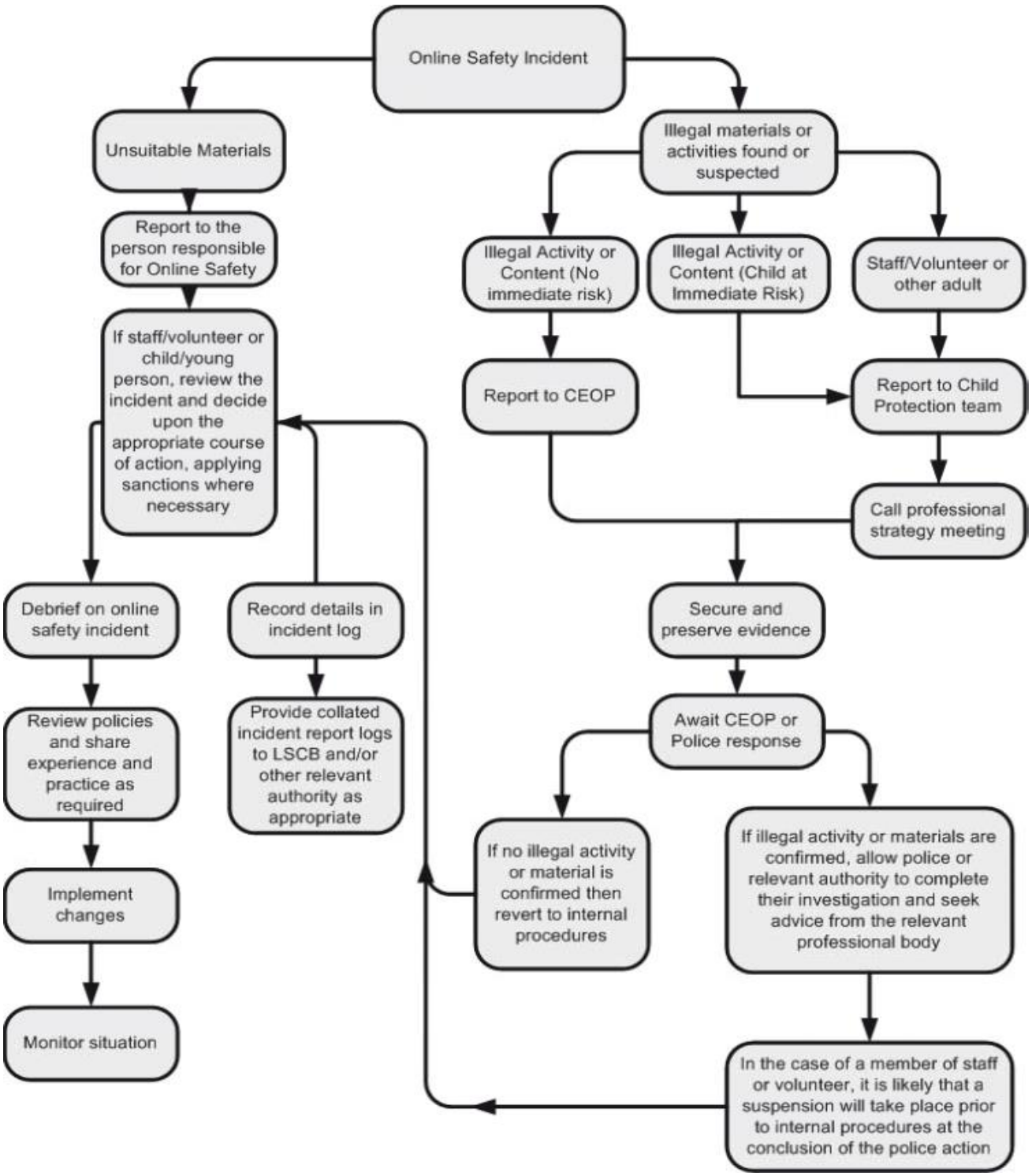
The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

	Line manager	Head Teacher	Local Authority / HR	Police	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).		X	X	X	X		X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
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	X	X			X	X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	X		X
Deliberate actions to breach data protection or network security rules	X	X	X		X	X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X				X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X				X	X	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X			X			
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X					X		
Using proxy sites or other means to subvert the school's filtering system	X				X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X
Breaching copyright or licensing regulations	X					X		
Continued infringements of the above, following previous warnings or sanctions	X	X			X			X

Reporting of Online Safety Breaches

It is hoped that all members of the school community will be responsible users of technology, 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:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in this policy.



Use of Handheld Technology (Personal phone 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
    - Members of staff are free to use these devices outside teaching time.
    - A school mobile phone is available for all professional use (for example when engaging in off-site activities) and members of staff should not use their personal device for school purposes except in an emergency or to contribute to the smooth running of the activity.
    - Staff in Nursery and Reception should have mobile phones locked away during teaching sessions
    - Pupils below Year 6, are not currently permitted to bring their personal phones or hand-held devices into school. Year 6 pupils must hand their devices into the office where they will be kept in a secure place until the end of the school day.

Personal hand-held technology	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	X							X
Use of mobile phones in lessons				X				X
Use of mobile phones in social time		X						X
Taking photos on personal phones or other camera devices				X				X
Use of hand held devices e.g. PDAs, gaming consoles	X						X	

Use of Communication Technologies

Email

Access to email is provided for all users in school via Microsoft Office 365 using their school email accounts. In addition, messaging (and email for staff) is available through the school's learning platform.

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)
- 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 permission / 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
- 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 they must not respond to any such email.

Use of Email	Staff / adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Use of personal email accounts in school / on school network	x							x
Use of school email for personal emails		x						x

Social Networking (including chat, instant messaging, blogging etc)

Use of social networking tools	**Staff / adults**				**Pupils**			
	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				X				X
Use of non educational instant messaging				X				X
Use of non educational social networking sites				X				X
Use of non educational blogs				X				X

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.**
- 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

See also the following guidance on publication of photographs

Use of Web-Bases Publications Tools

Website

Our school uses the public facing website www.bewdleyprimary.co.uk only 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 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.
- 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 a website or blog, and never in association with photographs
    - where possible, photographs will not allow individuals to be recognised
    - written permission from parents or carers will be obtained before photographs of pupils are published on the school website
    - All posts on the website will fully comply with GDPR regulations.
    - Pupil's work can only be published with the permission of the pupil and parents or carers.

Professional Standards for Staff Communication

In all aspects of their work in our school, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012. Teachers translate these standards appropriately for all matters relating to online safety.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform 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.

Infrastructure

Password Security

The school's online 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. We also have a level of filtering protection implemented by our school technician.

It is recognised that the school can take full responsibility for filtering on site but current requirements do not make this something that we intend to pursue at this moment.

Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the Headteacher. She manages 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 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 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

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

Staff users will be made aware of the filtering systems through briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through online safety awareness sessions / newsletter / parent workshops etc.

Changes to the Filtering System

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the headteacher.
- The Headteacher checks the website content to ensure that it is appropriate for use in school.
- If agreement is reached, the Headteacher makes a request to the in school technician. If it is beyond their filtering system, then contact is made with the Broadband team.
- The Technician/Broadband helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions.
- School Improvement Service Learning Technologies staff may then be notified of websites that have been unblocked to review them in partnership with the Broadband Team. If sites are found to not be appropriate, access will be discussed with the school and then removed.

The headteacher will need to apply a rigorous policy for approving / rejecting filtering requests and should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

Monitoring

ZuluDesk is used to monitor all laptops and iPads in the school. The Business Manager and online safety co-ordinator have access and conduct weekly checks.

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 as follows:

- Identified member(s) of staff reviews the monitoring 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 (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

Audit/Reporting

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

- the online safety governor
- the Worcestershire Safeguarding Children Board on request
- School Technician

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

EDUCATION

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 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.

Online Safety education will be provided in the following ways:

- A planned online safety programme is provided as part of Computing, PHSE and other lessons. This is regularly revisited, covering the use of technologies both in school and outside school
- Key online safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- 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 pedigree of the compilers / owners of the website
    - See lesson 5 of the Cyber Café Think U Know materials below
    - 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 online 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 – including non-teaching staff - receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: The Headteacher will be CEOP trained.

- The Headteacher will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- All teaching staff are aware of the content of the Online Safety Policy
- The Headteacher will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

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 IT, 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 School Improvement 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 headteacher 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 evening and parents' online safety meeting/workshops