E-Safety Policy
Pendock C E Primary School

A: Policy and Leadership

This section begins with 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 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**

The school council regularly discusses issues relating to e-safety and when appropriate invite the school E-safety Co-ordinator to attend meetings. 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's Board.

1. Responsibilities:
E-safety Co-ordinator, Governors, Head, Classroom based Staff, IBS

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

a. The E-safety coordinator :

- Takes day to day responsibility and has a leading role in establishing and reviewing the school e-safety policies;
- Ensures 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 all staff
- Liaises with the Local Authority
- Liaises with IBS
- Meets with Head as appropriate to discuss any issues
- Attends relevant meetings and committees of Governing Body
- Receives appropriate training and support to fulfil their role

b. 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 meeting with the Head and Policy Central Monitor on a regular basis to monitor incident logs and to be able to report back to the governing body.

c. Headteacher:

- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Reviews weekly with Policy Central Monitor the output from monitoring software and initiates action where necessary.

The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school, though the day to day responsibility for e-safety is delegated to the e-safety coordinator.

The Headteacher 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 (see flow chart below and other relevant Local Authority procedures).

d. Classroom based Staff

Teaching and support staff are responsible for ensuring that:

- 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 (see Appendix 1)
- They report any suspected misuse or problem to the E-Safety Co-ordinator/Head
- They undertake any digital communications with pupils in a fully professional manner and only using official systems (see Professional standards for staff communication below)

e. IBS

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 outlined in IBS' School's System and Data Security Policy (and any relevant Local Authority E-Safety Policy and guidance).

2. Policy Development, Monitoring and Review

The e-safety policy has been developed and based on the Worcestershire County Council's model policy by the:-

- Head teacher
- E-safety Co-ordinator
- Support Staff
- Governors
- Parents
- Pupils

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

- Staff meetings
- School council
- Governor's meeting
- Parents meetings
- School newsletters

Schedule for development/monitoring/review of this policy

Approved by the governing body on:	**January 2017**
The implementation of this policy will be monitored by:	The Head, E-Safety Co-ordinator and Future Cloud (formerly Policy Central) Monitor
Monitoring of this policy 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 monitoring group (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding	Termly
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 2018 July 2019 July 2020
Should serious e-safety incidents take place, the following external persons/agencies should be informed:	• WSCB • LA Designated Officer • Worcestershire Senior Adviser for Safeguarding Children in Education • West Mercia Police

3. Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers to such extent as is reasonable to regulate the behaviour of the pupils when they are off 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 the 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.

4. Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to school systems.

AUA are provided in Appendix 1 of this policy for:-

- Pupils
- Staff (and volunteers)
- Parent/carer volunteers

AUA are signed by all pupils as they enter the school with parents signing on behalf of children below Year 2 when necessary.

Pupils re-sign on an annual basis.

All employees of the school, and volunteers, sign when they take up their role and in the future if significant changes are made to the policy.

Parents sign if they take up a volunteering position that involves using the Internet and in the future if significant changes are made to the policy.

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

5. Self-Evaluation

Evaluation of e-safety is an ongoing process and links to other self-evaluation tools used in school and informs the school's judgement on its ability to keep pupils safe. The views and opinions of all stakeholders (pupils, parents, teachers, and governors) are taken into account as a part of this process.

6. Whole School approach and links to other policies

Core ICT policies:

IT 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)	How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the e-safety policy.
Computing Curriculum and/or Worcestershire Primary ICT progressions	Key documents and associated resources directly relating to learning covering the computing curriculum.

Other policies relating to e-safety

Anti-bullying	How the school strives to eliminate bullying – link to cyber-bullying
PSHE	E-safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of E-Safety. ***The e-safety policy forms 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, academies and settings**

7. Illegal or Inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in an education 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, transfer data, 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 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
- On-line shopping/commerce unless directly related to school business

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. See Appendix 2.

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 and Staff Sanctions

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Students

Category A infringements

• Use of non-educational sites during lessons
• Unauthorised use of email
• Unauthorised use of mobile phone (or other new technologies) in lessons
e.g. to send texts to friends
• Use of unauthorised instant messaging / social networking sites
[Possible Sanctions: referred to class teacher / e- Safety Coordinator/ Headteacher/removal of phone]

Category B infringements

• Continued use of non-educational sites during lessons after being warned
• Continued unauthorised use of email after being warned
• Continued unauthorised use of mobile phone (or other new technologies) after being warned
• Continued use of unauthorised instant messaging / chatrooms, social networking sites,
• Use of File sharing software
• Accidentally corrupting or destroying others' data without notifying a member of staff of it
• Accidentally accessing offensive material and not logging off or notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / Headteacher/ removal of Internet access rights for a period / removal of phone / contact with parent]

Category C infringements

• Deliberately corrupting or destroying someone's data, violating privacy of others
• Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
• Deliberately trying to access offensive or pornographic material
• Any purchasing or ordering of items over the Internet
• Transmission of commercial or advertising material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Headteacher / removal of Internet and/or Learning Platform access rights for a period / contact with parents / removal of equipment]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform LA as appropriate

Category D infringements

• Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
• Bringing the school name into disrepute

[Possible Sanctions – Referred to E safety coordinator and Headteacher / Contact with parents / possible exclusion / removal of equipment / refer to Police / LA e- safety officer]

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

• Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
• Misuse of first level data security, e.g. wrongful use of passwords
• Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - referred to E safety Coordinator/ Headteacher - Verbal Warning to be given.]

Category B infringements (Misconduct)

• Accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;

[Sanction - referred to E Safety Co-ordinator / Headteacher. Written/Verbal Warning given.]

Category C infringements (Gross Misconduct)

• Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
• Repeated infringements of Category B;
• Accessing or storing inappropriate images of children;
• Any deliberate attempt to breach data protection or computer security rules;
• Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
• Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
• Bringing the school name into disrepute.
[Sanction – Referred to Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police]

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff is alleged to have committed a serious act or acts of gross misconduct they should be instantly suspended. There will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken. Schools will involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

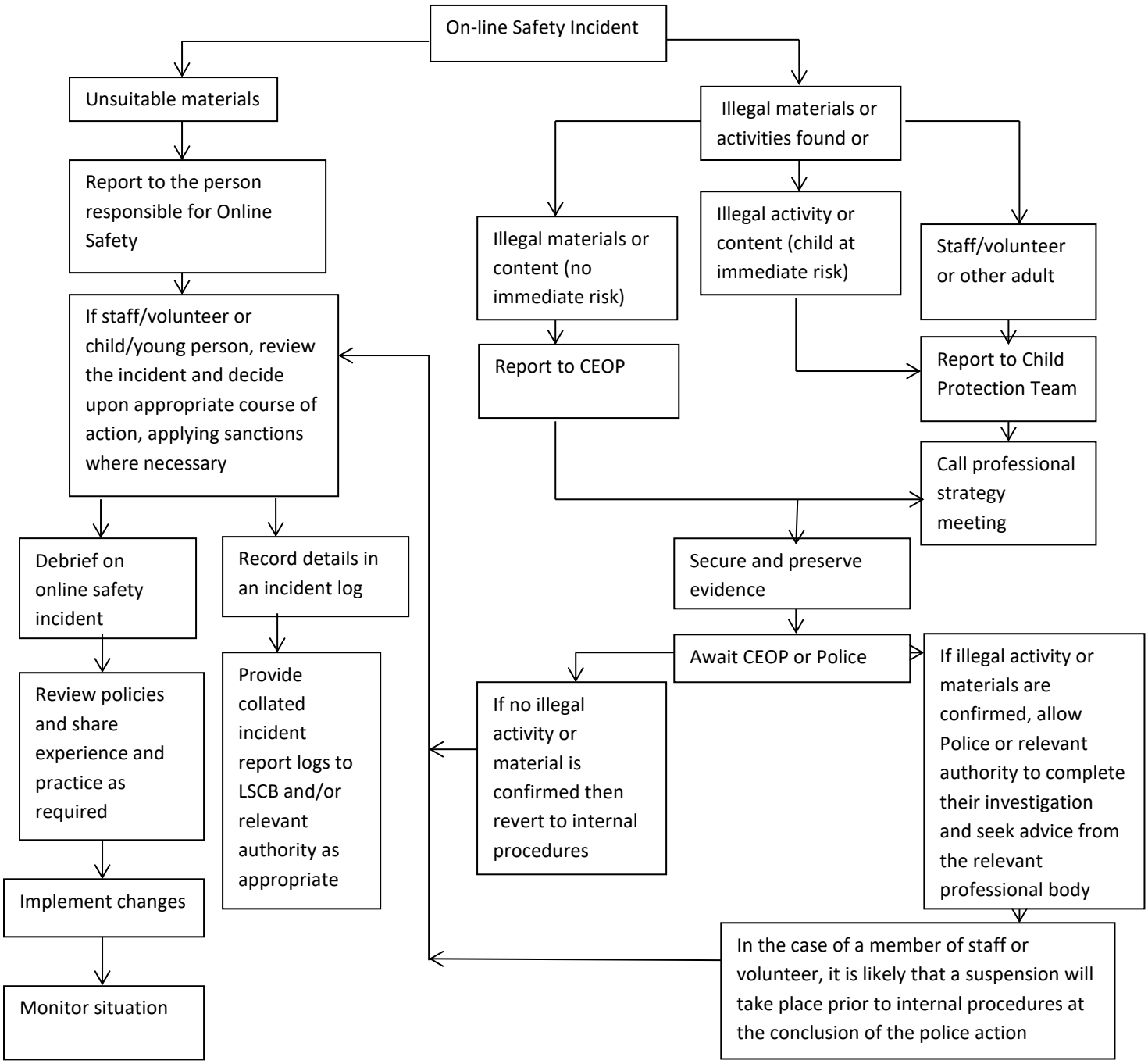
Child Pornography found?

In the case of Child Pornography being found, the member of staff should be immediately suspended and the Police should be called.
Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):
http://www.ceop.gov.uk/reporting_abuse.html

8. Reporting of e-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, 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 section 7 of this policy.



9. Use of hand held technology

We set out below our current policy but recognise that the area of mobile technology is advancing rapidly and will endeavour to review our policies on a regular basis to reflect this.

- Staff may bring their mobile phones and devices into school but they may not be used in the classroom and may not be used to photograph or video children. Every member of staff has signed an Agreement to reflect this policy
- Members of staff may use their phone in an emergency situation.
- Pupils may bring iPads into school for the specific purpose of sharing homework in class but they must be kept in the school office during the day and returned to pupils at the end of the day
- School iPads are used in the classroom with the appropriate supervision
- School mobile phones are available for staff to use on educational visits
- If a child brings a mobile phone to school it is to be stored in the school office until the end of the school day.

10. Use of communication technologies

a. Email

Access to email is provided for all schools using the Worcestershire Learning Gateway via their global ID's.

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

- Pupils should use only the school email services to communicate with others regarding school business when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- 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 (see Education section in this policy)
- Users must immediately report to their teacher/e-safety coordinator – in accordance with this policy – the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.

b. Social Networking

The use of social networks is not permitted within school.

11. 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. (see section on Education below). In particular they should recognise the risks attached to publishing their own images on the internet e.g. social networking sites.

Members of staff are allowed to take digital still and video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images. Such images must be taken on school devices only.

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.

Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph. If in doubt, staff should check the record on Class Registers.

Pupils must not take, share, publish or distribute images of others without their permission

See below for further guidance on publication of photographs.

12. Use of web-based publication tools

Website

Our school uses the website http://www.pendockprimary.co.uk/ only for sharing information with the community beyond our school. This includes, from time to time, celebrating work and achievements of pupils. 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)
- Pupils' names will not be used on the website.
- 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' names will not be used anywhere on a website or blog.
    - 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
- A pupil's work can only be published with the permission of the pupil and parents or carers.

13. Professional standards for staff communication

In all aspects of their work in our establishment, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012:

http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf

Teachers translate these standards appropriately for all matters relating to e-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
- 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 teaching and learning. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

B: Infrastructure

14. Password security

All staff must ensure that sensitive information is physically secured or password protected.
In order to minimise the risk involved in accessing the IT systems users are required to adhere to the following:

- Always follow your school's password policy
- Always log out, or "lock" the screen when leaving your computer unattended
- 'Strong' passwords should be used – don't use simple or obvious passwords
- Never share passwords with others, never tell your password to anyone
- Never write passwords down and leave them near the computer
- Don't use work passwords for personal online accounts
- Don't save passwords in web browsers
- Never use your user name as a password
- Never email your password or use it in an instant message

It is your personal responsibility to ensure your device is kept secure, in accordance with the following guidelines.

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see Section C "Education" of this policy).

15. Filtering

a. 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. No filtering system can, 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 preventive measures which are relevant to the situation in this school.

As a school buying broadband services procured by Worcestershire County Council, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

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.

b. Responsibilities

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

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Worcestershire, or other, school filtering service:

All users have a responsibility to report immediately to teachers/e-safety co-ordinator any infringements of the 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.

c. Education/training/awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme (see Section C of this Policy).

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

- Signing the Acceptable Use Agreement
- Briefing in staff meetings, training days, memos etc. (timely and ongoing)

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

d. 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 Headteacher or E-Safety Co-ordinator.
- The Headteacher/Coordinator checks the website content to ensure that it is appropriate for use in school.

THEN

- If agreement is reached, the Headteacher/Co-ordinator makes a request to IBS schools Broadband Team, or other filtering provider
- The team 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 well in advance of teaching sessions.

The Headteacher will need to apply a rigorous policy for approving/rejecting filtering requests. This can be found in Appendix 3 but the core of this 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.

e. Monitoring

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

Monitoring takes place as follows:

- Identified members of staff (Headteacher/E-safety Co-ordinator and Policy Central Monitor) review the monitoring console captures in turn, weekly.
- 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 Egyptians, or 'stabbed' when studying the Romans) so the word can be allowed for the period the topic is being taught.

f. Audit/reporting

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

- The e-safety governor within the timeframe stated in section A – governor responsibilities
- 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.

16. Technical Security

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

17. Personal data security (and transfer)

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

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see Section C of this policy).

C: Education

18. 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 constant help

and support to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping them 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 Computing, PSHE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and beyond school.
- 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 (see Appendix 1) and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- In lessons where internet use is pre-planned, it is best practice that younger pupils should be guided to sites checked as suitable for their use. Processes should be in place, and known to pupils, 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 pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support necessary.
- Pupils will be made aware of what to do should they experience anything, while on the internet, which makes them feel uncomfortable

a. 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 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
    - Referring to other (including non-digital) sources

- Pupils will be taught to acknowledge the source of the 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/. These are shared by a CEOP trained teacher.

b. The contribution of the pupils to the e-learning strategy

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

19. Staff Training

It is essential that all staff - including non-teaching 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.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- 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 Agreement which are signed as part of their induction.
- The E-Safety Co-ordinator will be CEOP trained.
- The E-Safety Co-ordinator will receive regular updates throughout through attendance at local authority or other training sessions and by reviewing guidance documents released by the DFE, the local authority, Ofsted, the WSCB and others.
- All teaching staff have been involved in the creation of this policy and are therefore aware of its content
- The E-Safety Co-ordinator will provide advice, guidance and training as required to individuals on an ongoing basis
- External support for training, including input to parents, is sought from appropriately qualified persons when required.

20. Governor training

Governors should take part in e-safety training /awareness sessions with particular importance for those who are members of any sub-committee or group involved in ICT, e-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 information sessions for staff and parents.

The E-safety Governor works closely with the E-safety Co-ordinator and reports back to the full governing body (see point 1 above, Responsibilities: Governors)

21. Parent and carer awareness training

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 their 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 should so 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, school website
- Parents evenings
- Feedback from the children

22. Wider community understanding

Messages to the public around e-safety should also be targeted towards grandparents and other adults engaging with pupils. Everyone has a role to play in empowering young people to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep them safe in the non-digital world.

Community users who access school ICT systems/website/learning platform as part of extended school/academy provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

Ratified by the Governing Body on 9th February 2017
Annual Review: Summer 2018
Next due: Summer 2019

Appendix 1

Acceptable use agreement for Pupils

Computer and Internet Use Agreement 2017/18

This agreement helps us to be fair to others, and to keep everyone safe when using the School Computer System and the Internet. It has been agreed by the School Staff, Governors, parents/carers and children.

Children's Responsibilities

- The School Council will help to develop our Acceptable Use Policy.
- I will ask before I use the internet, as it is a public place.
- I will only look at my own files, or those in the shared areas.
- I will ask an adult before I bring software, disks or memory sticks into school.
- I will only email people who are approved by school or my parents.
- Anything I write will be polite and respectful.
- I will never give my home address or my phone number to anyone
- I will never meet anyone from the Internet.
- I must tell an adult if I get an email or attachment from someone I do not know before I open it.
- If I see anything that I am unhappy with or unsure of, I will tell an adult immediately.
- The school may check my files, Internet sites I have visited and emails.
- I understand that if I break these rules, I may not be allowed to use the Internet and computer facilities of the school.

Parent/Carer's Responsibilities

- I will read and sign this Computer and Internet Use Agreement.
- I have/will attend a Parent's Internet Safety meeting at School.
- I will closely monitor all devices with internet access and will consider using the appropriate filters.
- I will promote healthy use of the Internet.

School's Responsibilities

- We will provide a yearly information evening on Internet Safety for all parents.
- We will make training and advice on using parental controls and firewalls available for parents.

The school may exercise the right to monitor the use of the school's computer and Internet systems, including access to web-sites, interception of email and deletion of inappropriate materials where the school believes unauthorised or criminal use of the school's computer and Internet system is, or may be, taking place. By the Parent/carer signing this policy, he/she is agreeing to his/her child's use of the school computer system and Internet facilities.

Signed: Child:_____ Print Name_____

Signed: Parent/Carer:_____ Print Name_____

Signed: Headteacher:_____ Print Name_____

Acceptable use agreement for staff and volunteers

The computer system is owned by the school and is made available to children to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy had been drawn up to protect everyone in school who uses the internet – children, staff, governors and parents.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

Staff requesting internet access should sign a copy of the Acceptable Internet Use Policy and return it to the ICT Co-ordinator.

- All internet activity should be appropriate to staff's professional activity or to the children's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received.
- Be aware of unsolicited e-mail from unknown parties. A reputable internet service is subscribed to by the school to try to avoid receipt of offensive materials.
- Use for personal gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected, as with any materials.
- Treat publishing on the internet in the same way as any other form of publication, for example, always seek parental permission before publishing photographs of children, whether named or anonymous.
- Posting anonymous messages and forwarding chain letters is not allowed.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Never give out information on the internet which could lead to the identification of a child by revealing their surname, address or other identifying details. This applies to e-mails and web publishing as well.
- Use of the network to access inappropriate materials such as pornographic, racist, illegal or offensive materials is forbidden.

Signed..... Date.....

Access granted..... Date.....

Acceptable use agreement for Parent/Carer volunteers (when use of the internet is involved) similar to above agreement except for blue

The computer system is owned by the school and is made available to children to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy had been drawn up to protect everyone in school who uses the internet – children, staff, governors and parents/carers.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any internet sites visited.

Volunteers requesting internet access should sign a copy of the Acceptable Internet Use Policy and return it to the ICT Co-ordinator.

- All internet activity should be appropriate to a volunteer's professional activity or to the children's education and an appropriate member of staff should supervise such activity
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mail being received.
- Be aware of unsolicited e-mail from unknown parties. A reputable internet service is subscribed to by the school to try to avoid receipt of offensive materials.
- Use for personal gain, gambling, political purposes or advertising is forbidden.
- Copyright of materials must be respected, as with any materials.
- Treat publishing on the internet in the same way as any other form of publication, for example, always seek parental permission before publishing photographs of children, whether named or anonymous.
- Posting anonymous messages and forwarding chain letters is not allowed.
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Never give out information on the internet which could lead to the identification of a child by revealing their surname, address or other identifying details. This applies to e-mails and web publishing as well.
- Use of the network to access inappropriate materials such as pornographic, racist, illegal or offensive materials is forbidden.

Signed..... Date.....

Access granted..... Date.....