USWORTH COLLIERY
PRIMARY SCHOOL

E Safety Policy

Designated members of staff: Gary Wright.

Chair of Governors: Alison Logan

What is an e-safety policy?

The E-Safety Policy is part of the School Development Plan and relates to others including those for ICT, Anti-Bullying and Safeguarding. This E-Safety Policy replaces the previous Internet Access Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole. E-safety encompasses not only Internet technologies but also electronic communications such as mobile phones, tablets and other wireless devices.

Why have an e-safety policy?

It highlights the need to educate children and staff about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. Anyone can send messages, discuss ideas and publish material with very little restriction. These features make it an invaluable resource used by millions of people every day. However, much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism – access to which would be more restricted elsewhere. Pupils must also learn that publishing information could compromise their security and that of others.

Why is use of the Internet important in supporting learning?

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

How does the Internet benefit education?

Benefits of using the Internet include:

- Access to world-wide resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- Cultural, vocational, social and leisure use in libraries, clubs and at home
- Access to experts in many fields for staff and pupils
- Staff professional development through access to national developments, educational materials and good curriculum practice
- l developments, educational materials and effective curriculum practice;
- Communication with support services, professional associations and colleagues
- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the Local Authority and DfE.
- Access to learning wherever and whenever convenient.

How will Internet use enhance learning?

- School Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information to a wider audience
- Internet access will be planned to enrich and extend learning activities as an integrated aspect of the curriculum

- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity
- Pupils will use the internet discerningly to answer key questions and follow lines of enquiry.
- Pupils will be apprised of suitable websites and will be educated in taking responsibility for Internet access.

How will pupils learn to evaluate Internet content?

- The school will ensure that the use of the Internet derived materials by staff and pupils complies with copyright law
- Pupils will be taught the importance of cross-checking information before accepting its accuracy and to question the value and credibility of the information
- Pupils will be taught how websites are ranked when using search engines and how to avoid the bias and manipulation that is possible in the way results are presented
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protection.
- Staff will be made aware of how to report unpleasant Internet content; informing the ICT Lead Teacher or a member of the senior management team directly who will contact BT (as Internet Service Provider (via Informative IT)
- Pupils will be informed that checks are made on files held on the system as part of the school's work with the Internet Service Provider to ensure that pupils are protected
- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television.

How will Internet Access be managed?

- School ICT security and filtering systems provided by Smoothwall will be regularly reviewed and upgraded.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.

How will Removable Media and Hand-Held Devices be managed?

Removable media refers to anything that can be used for taking electronic information out of school. This includes USB sticks; memory cards etc but is not limited to CD and DVD burning. Also, many consumer electronic gadgets such as mobile phones, PDA's and tablets (iPads) can be used for removable data storage.

Memory sticks or USB sticks are convenient to carry but this also makes them easy to become lost or stolen. A memory stick can contain thousands of documents and large databases. Whole directories can be put onto the stick without checking exactly which files are being copied and what their individual security classification is. It is also possible that if the stick is taken away and used on a virus infected PC, many corrupted documents may then be put back onto the school network.

Rules about the use of Removable Media of Hand-Held Devices

- Staff must ensure that portable storage devices are encrypted if they include sensitive, confidential or personally identifiable information. All staff members have been issued with encrypted USB pens and these must be used to store any data or information of any kind relating to their pupils. Good practice dictates that all data which refers to individuals or contains sensitive information of any kind should be encrypted
- Staff must obtain approval from a member of the Senior Management Team or the Head Teacher before creating, moving or copying information, files, folders etc… onto a portable storage device
- Staff should ensure that portable devices are stored securely when left unattended
- Staff should ensure that portable technology such as the iPads are password protected.

- Staff should ensure that devices taken off-site should not be left unattended in public places or at an individual's home address
- To avoid total loss of data, users are to ensure that information stored on the portable devices is 'backed-up' and held in the appropriate place on the school network
- If a portable storage device or hand-held device is lost, stolen or mislaid staff must report it immediately to the Head Teacher and where appropriate ICT Engineer.
- Staff should only use equipment that has been purchased or approved by the Head Teacher.
- Staff are responsible for ensuring that visitors or contractors who bring their own USB devices into school (to give a presentation for example) are supervised at all times while the device is connected to school equipment.

E-mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, e-mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- Pupils may only use approved e-mail accounts on the school system (Office 365).
- Pupils must immediately tell a member of staff if they receive offensive or inappropriate content.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school should consider how e-mail from pupils to external bodies is presented and controlled.
- E-mail sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The sending of abusive or inappropriate email messages is forbidden.

Social Networking and E-Communication

Conferencing applications offering the instantaneous exchange of text between users have great potential for education and provide a basis for pupils' understanding of global citizenship as they encounter different societies and cultures. Detailed guidance for staff is provided in the LA Safeguarding Document.

- Pupils will not be allowed access to public or unregulated chat rooms
- They will be closely supervised during well-planned activities and the importance of chat room safety clearly emphasised
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Newsgroups will not be made available unless a specific educational requirement for their use has been demonstrated
- Risk assessment will be carried out before pupils are allowed to use emerging technologies in school
- Pupils will use only moderated and carefully selected E-Communication sites, e.g. Ranger Remote, Hector's World.
- Pupils and parents will be advised on how to safely utilise social networking spaces outside school
- Mobile phones will not be used during lessons or school session times. Staff are provided with a locker for the storage of mobile phones as they are not permitted in classrooms or other areas of the school where there are pupils.

Publishing on the Web

A Website is the ideal way to promote our school, celebrate good work, to inform parents/carers and to publish resources useful for homework. It is important that the Website reflects our ethos, information is correct, and that pupils and staff are protected.

- Staff or pupil personal contact information will not generally be published
- Personal data will be recorded, processed, transferred and made available according to GDPR.
- Photographs that include pupils will be carefully selected so that individual pupils without the appropriate consent cannot be identified or their image misused
- Group photographs will not have name lists attached
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the website or other online space and parents/carers should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories
- Work can only be published with the permission of the pupil and parents/carers
- Work must be the author's own and credit any other work included
- The Head Teacher will delegate responsibility to an identified member of staff to ensure that content is correct and quality of presentation is maintained
- The point of contact on the Website will be the school's address and telephone number
- Home information or individual e-mail identities will not be published.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to GDPR.

Managing videoconferencing & webcam use (via iPads)

The following guidelines must be adhered to if using webcam facilities in school:

- Pupils must ask permission from the supervising teacher before using the webcam
- Webcam use will be appropriately adapted to the pupils' age
- Video conferencing should use the educational broadband network to ensure quality of service and security

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of mobile technology, such as iPads, will be monitored regularly.
- Parents and pupils will also agree to a set of terms of conditions before access to school technology is granted (Acceptable Use Policy).
- Staff will agree to a set of terms of conditions before access to school technology is granted (Appendix V, VI & VII).

How will Internet access be authorised?

It is essential that all staff and pupils are aware of the need for safety when accessing the Internet.

- All staff, including supply staff, classroom assistants and support staff will be provided with the E-Safety Policy and its implications discussed.
- Visitors using the Internet with pupils must sign an *Acceptable Internet Use Statement for Staff and accept the Staff Code of Conduct* (see appendix IV & VII) before using the Internet in school
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- Rules for Responsible Internet use will be displayed in poster format in all rooms where computers are used (see appendix IX).
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials
- At Key Stage 2, supervised Internet access will be granted to a whole class or individual pupils who have demonstrated their understanding of and compliance with *The Acceptable Use Policy,*
- Parents/carers will be asked to sign and return a permission form (*Rules for Responsible Internet Use*) allowing pupils supervised Internet access where beneficial to their education (see appendix VI, VII, VIII).

How will risks be assessed?

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor the LA can accept liability for any material accessed, or any consequences of Internet access.

- The school will audit ICT use (*via Smoothwall Reports*) to establish if the E-Safety Policy is adequate and that the implementation of the E-Safety Policy is appropriate and effective.
- Senior staff will ensure that regular checks are made to ensure that filtering methods selected are appropriate, effective and reasonable.

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content so the school will work in partnership with parents, the LA, the DFE and private providers (*Informative Solutions*) to ensure systems re reviewed and improved.

How will E-Safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaints about staff misuse must be referred to the Head Teacher.
- Pupils & parents will be informed of the complaints procedure policy.
- Pupils & parents will be informed of consequences for pupils misusing the Internet.
- Sanctions for irresponsible use will be linked to the school's Behaviour Policy and may involve a pupil being denied Internet access for a specified period.
- Discussions may be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.
- Complaints of a Child Protection nature must be dealt with in accordance with school Safeguarding procedures.

How will we enlist the support of parents and carers?

Internet use in the home is now common. Not all parents exercise the same level of supervision over their children's Internet use and the sites they access. In order to protect pupils:

- Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school.
- The school will maintain a list of e-safety resources for parents and carers. (appendix iii)
- Drop in workshops will be held to inform and advise parents on the topic of E-Safety.

Author: P Arthur
Agreed date: December 2018
Implementation date: January 2019
Review Date: Every 3 years

Signed …… Date ……..
Head Teacher

Signed …… Date ……..
Chair of Governors

Rules for Responsible Use of ICT

The school computer system allows Internet access to enhance your learning.
Following these rules will help to keep you and others safe:

1. I will only access the system with my own Personal Login.
2. I will not access other people's files.
3. I will use school devices for school work and homework.
4. I will not bring in disks or memory sticks from outside school unless I have been given permission.
5. I will ask permission from a member of staff before using the Internet.
6. I will only use the email system to contact pupils within the school network or that my teacher has approved.
7. The messages I send will be polite and appropriate.
8. I will not give any personal details such as my home address, telephone number or home e-mail address or arrange to meet someone unless my parent, carer or teacher has given permission (e.g. school visit).
9. I will report any unpleasant material that appears on screen or inappropriate messages sent to me. I understand this report would be confidential and would help to protect other pupils and myself.
10. I understand that the school may check my virtual files and may monitor the Internet sites I visit.
11. I understand that only work and images agreed by my parents, carers or teachers will be published on the school website.

Signed: …… Signed: ……
Parent/Carer Pupil

Date: …….. Date: ……

Sample Letter to Parents/Carers

Dear Parents/Carers

As you are no doubt aware ICT is an essential element in 21st century life for education, business and social interaction. Computing is also part of the statutory curriculum and a necessary tool for staff and pupils. The school has a duty to provide students with safe and secure access to ICT resources as part of their learning experience. Use of ICT within the curriculum produces significant educational benefits including access to information from around the world and the ability to communicate widely and to publish easily.

In our school we provide a guided and balanced curriculum that is well-planned, task-orientated and educational within a regulated and managed environment in order to enrich and extend your child's learning activities. Directed and successful use of ICT also reduces the opportunities for activities of little educational value.

Access to emerging technologies is an entitlement and privilege for staff and students who show a responsible and mature approach to its use.

Within school, your child is able to access technology via a system which is filtered and monitored by the Local Authority and the school in order to protect them as much as possible from contact with inappropriate material. Email communication takes place within a restricted network so that messages can be monitored and only approved people can participate. Only work or images agreed by yourself and the school would be published on the website with your permission.

Children are made aware from a very early stage that there is a need for safety in their use of ICT, particularly with regard to the Internet, and are taught how to manage their use responsibly and to report any unpleasant experiences.

Should you have concerns about any aspect of your child's use of ICT, or to discuss our policy in more detail, please telephone school to make an appointment to do so.

We would be grateful if you would sign and return the enclosed *Rules for Responsible Use of ICT* form giving permission for your child to utilise school equipment and software to its fullest.

Yours sincerely,

Mr G. Wright
Head Teacher

Useful sites for parents/carers interested in safe internet use at home:

www.thinkyouknow.co.uk/
Take the quiz and see if you are a switched-on mum or digital dad!
Useful information for parents and children. The 5-7 year old section provides safety information in the form of some simple games. 8-10 year olds can visit the cyber café to help the on-screen characters stay safe. Information for 11-16 year olds is practical and straight-talking.

kidshealth.org/parent/positive/family/net_safety.html
A text-based site with lots of useful references to other sites dealing with children's issues.

www.kidsmart.org.uk/
A child-friendly site with drawings and information provided by children themselves. A good one to sit and use **with** your child so that you can talk through any issues together.

www.bbc.co.uk/parenting/your_kids/safety_internet.shtml
A single page outlining the main dangers of unsupervised internet use and what you can to do prevent danger or deal with problems if they occur. See also their page on Internet Safety rules you could agree to implement at home. **www.bbc.co.uk/schools/...at.../internet_safety_rules.shtml**

There are many more sites and also "firewall" products available to help reduce the chances of your children accessing inappropriate material when using the internet at home.

Appendix iv

Usworth Colliery Primary School
Acceptable Internet Use Statement for Staff

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.
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.

- Access must only be made via the authorised account and password, which must not be made available to any other person
- All Internet use should be appropriate to staff professional activity
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden
- Sites and materials accessed must be appropriate to work in school; Users will recognize materials that are inappropriate and should expect to have their access removed
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received
- The normal rules of social interaction apply to e-mail. The remoteness of the recipients must not be used to excuse anti-social behaviour: harassment, intimidation and bullying behaviour
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded
- Posting anonymous messages and forwarding chain letters is forbidden
- Copyright of materials and intellectual property rights must be respected
- Legitimate private interests may be followed, providing school use is not compromised
- Use for personal financial gain, gambling, political purposes or advertising is forbidden.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the Head Teacher for approval.

Full name … post … … … … … … … … … … … … … …

Signed … date … … … … … … … … … … … … … …

Access granted … date … … … … … … … … … … … … … …

Appendix V

Staff Electronic Device Agreement

Make:_____ Model:_____

Serial No._____ Device ID:_____

I acknowledge receiving the above School device and will use it appropriately and in line with the school Acceptable Use Policy and the recent Social Networking Policy which I have signed and agreed to.

With specific relevance to;

- Where it is intended to use social networking sites on mobile devices owned by the school, you should ensure you have received approval from a member of the SMT prior to undertaking such activities.
- Personal use of the internet, including access to social networking sites, will NOT be permitted on school based equipment in use in school either before or after work or during designated lunch periods. Non work related access during work time and whilst on school premises is not permitted.
- Usage of mobile devices at home should not involve any breach of copyright, or promote any financial, commercial, business, or political interests.
- When downloading personal apps, they must firstly be stored in a 'personal folder' and personal Apple IDs should be signed out immediately after use.
- Personal apps not installed by the school should not be accessed whilst on school premises.
- Any personal apps that require a log in must always be logged out before entering school premises.
- Shared devices, which are not solely intended for the use of one individual, should not have personal apps installed nor should they have personal or work email accounts set up on the device.
- Staff should be aware that all internet usage is monitored and stored on the device and should refrain from accessing personal banking accounts or similar for security purposes as they may be accessed by another individual.
- Passcodes set up by the school MUST not be removed or changed without prior permission.
- Mobile devices owned by the school must be brought in to school each day along with chargers and should be made available for random checks and maintenance.

Any damage to the device MUST be reported IMMEDIATELY to the Head teacher, ICT Co-ordinator or the IT Technician.

I understand that the device will remain the property of Usworth Colliery Primary School and that I am solely responsible for it and must return it to the school should my employment at the school terminate.

I agree to the above:

Signed: _____ Print Full Name: _____

Date: _____

Appendix Vi

Staff Laptop Agreement

Make:_____ ___ Model:_____ Serial No._____

I acknowledge receiving the above School Staff Laptop and will use it appropriately and in line with the school Acceptable Use Policy which I have signed and agreed to.
Any damage to the laptop MUST be reported IMMEDIATELY to the Head teacher, ICT Co-ordinator or the IT Technician.
I understand that the laptop will remain the property of Usworth Colliery Primary School and that I am solely responsible for it and must return it to the school should my employment at the school terminate.

I agree to the above:

Signed: _____ Print Full Name: _____

Date: _____

Staff Code of Conduct

Revised September 2018

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.

- I will ensure that my information systems use will always be compatible with my professional role.

- I understand that school information systems may NOT be used for private purposes whilst on school premises, e.g. accessing personal email accounts and personal internet use.

- I will use the email account that I have been issued with by the school for sending and receiving emails for work related purposes only and no other email accounts on school computers.

- I will only use the internet for work related purposes whilst at school or whilst logged into a school account using a school laptop.

- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

- I will respect system security and I will NOT disclose any passwords or security information to anyone other than an appropriate system manager.

- I will NOT download or install any software or hardware without prior permission.

- I will NOT plug in any portable storage devices (e.g. memory sticks) without having them scanned by the ICT Engineer prior to use.

- I will ensure that pupil's personal data is kept secure and is used professionally and appropriately within my role in school. I will NOT take pupil's personal data off the school premises without approval by the Headteacher first. I will ONLY store Pupil's personal data on the schools server and NOT on laptops, memory sticks or any other portable devices that are not encrypted.

- I will respect copyright and intellectual property rights.

- I will report any incidents of concern regarding children's safety to the school e Safety Coordinator or the Designated Child Protection Coordinator.

- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

- Network access must be made only via the user's authorised account and password, which must NOT be given to any other person.

- I will NOT leave computers/laptops/iPads logged on whilst unattended.

- I will NOT use chat rooms or any other form of social networking site whilst in school and will follow the guideline expressed in the school Acceptable Use Policy whilst at home.

- Use for personal financial gain, gambling, political purposes or advertising is NOT permitted.

The school may exercise its right to monitor and log the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

By clicking 'I Accept' you acknowledge reading and agreeing to comply with the School Acceptable Use Policy, GDPR Policies and the above Staff Code of Conduct and are aware of your responsibilities.

Appendix Viii

Pupil Code of Conduct

Revised September 2018

We ask permission before using the internet.

We only use websites our teacher has chosen.

We turn off the screen and tell an adult immediately if we see anything we are uncomfortable with.

We only email people an adult has approved.

We only send e-mails that are polite and friendly using the email account that the school has given me.

We do not open e-mails sent by anyone we don't know.

We never give out personal information or passwords.

We never arrange to meet anyone we don't know.

We do not use Internet chat rooms.

I agree to the above school rules

Appendix IX

Rules when using the ICT room

1) I will only use my own Login.

2) I will not open or change other people's work.

3) I will only use school computers for school work and homework.

4) I will not bring in disks or memory sticks from outside school unless I have been given permission.

5) I will ask before using the Internet.

6) I will only use my school email address to message pupils from this school or people my teacher has approved.

7) The messages I send will be polite and appropriate.

8) I will not give any personal details such as my home address, telephone number or home e-mail address or arrange to meet someone unless I have been given permission to do so (e.g. school visit).

9) I will report anything inappropriate that appears on screen or is sent to me.

10) I understand that the school may check my files and the Internet sites that I visit.