

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

Signed and dated:
Headteacher
Chair of Governors

WHAT IS E-SAFETY?

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Policy has been extensively revised and renamed as the Schools' E-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

SEXTING

'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. Bredenbury Primary School takes a proactive approach to help students to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

Rewritten in:	February 2016
Reviewed by co-ordinator in:	June 2017
Ratified on:	3.7.2017
To be reviewed annually:	
Reviewed by staff and governors in:	October 2020
To be reviewed by staff and governors in:	October 2021
The e-safety co-ordinator is:	Mrs S McAtear
The e-safety Governor is:	Mr T Hayes

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

SAFEGUARDING

Bredenbury Primary School has a duty of care and responsibility towards pupils, parents/carers and staff. The care and safety of the individual is the key issue behind this document. Bredenbury Primary School believes that the use of information and communication technologies in schools brings fantastic benefits. However recognising issues around e-safety and planning accordingly will help ensure appropriate, effective and safer use of electronic communication.

We work together with governors, staff, pupils, parents and carers to create a community which values the use of new technologies in enhancing learning, enhancing learning, encourages responsible use of computers and follows agreed policies to minimise potential e-safety risks.

Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use the internet at school.

CORE PRINCIPLES OF E-SAFETY

E- safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

BACKGROUND

New technologies have become integral to the lives of children and young people in today's society, both educationally and socially. The internet and other digital technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps staff and pupils learn from each another. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The requirement to ensure that young people are able to use the internet and related communications appropriately and safely is addressed as part of the wider

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

duty of care to which we all work. This e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education plus the child themselves.

The use of these exciting and innovative tools in educational establishments and at home has been shown to raise educational standards and promote pupil/student achievement. However, the use of these technologies can put young people at risk within and outside school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of /sharing of personal information
- 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
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloads of music or videos
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world and it is essential that this e-safety policy is written in conjunction with our policies on Child Protection, Behaviour, Special Educational Needs, Health and Safety, Anti-Bullying and in accordance with our Equality and Accessibility Plans.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build young peoples' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

SCOPE OF THE POLICY

This policy applies to all members of school who have access to and are users of schools ICT systems, both in and out of the school. The Education and Inspection Act 2006 empowers Headteachers, to such extent as reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by the policy, which may take place out of the school but are linked to membership of the school.

The school will deal with such incidents within the policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of the incident.

WHAT DOES ELECTRONIC COMMUNICATION INCLUDE?

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs, Wikis and Tweepers
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- I pads
- Other mobile devices with web functionality

At Bredenbury Primary School, we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

INTRODUCTION/APPLICATION OF THE POLICY

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

- The e-safety policy will be introduced to the pupils at the start of each school year.
- E-safety posters are prominently displayed.
- Safety rules will be posted in rooms with Internet access;
- Pupils will be informed that network and Internet use will be monitored;

- Safety training will be introduced to all to raise the awareness and importance of safe and responsible internet use;
- Instruction in responsible and safe use should precede Internet access;
- An e-safety module will be included in the PSHE, Citizenship or ICT programmes covering both school and home use;
- All staff will be given the School e-Safety Policy and its application and importance explained;
- Staff should be aware that Internet traffic can be monitored and traced to the individual user;
- Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues;
- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school website and on the school learning platform; • Internet issues will be handled sensitively, and parents will be advised accordingly

ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The Headteacher is the e-Safety co-ordinator in our school.

Governors:

The role of the e-safety governor will include:

- Regular meetings with the e-safety co-ordinator
- Ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering
- Reporting back at Governor meetings

Head of School:

- The Head of School has a duty of care for ensuring the safety (including e-safety) of members of the school community and is the delegated e-safety co-ordinator
- The Head of School and another senior member of staff should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff
- The Head of School is responsible for ensuring that as the E-Safety Co-ordinator they receive suitable training to enable them to carry out their e-safety roles and to train other colleague

E-Safety Co-ordinator (the Headteacher):

The role of the E-Safety Co-ordinator will include:

- Takes day to day responsibility for e-safety issues as well as 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 taking place
- Provides training and advice for staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- Meets regularly with the E-Safety Governor

Technical Staff:

The role of the technical staff will include:

- Ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- Ensuring that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply
- Ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- Making sure they have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- Ensuring that they have read, understood and signed the Staff Acceptable Use Policy
- Ensuring that they report any suspected misuse or problem to the Headteacher (E-safety Co-ordinator) for investigation / action / sanction

Teaching and Support Staff:

The role of the teaching and support staff will include:

- Having an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- Ensuring they have read, understood and signed the Staff Acceptable Use Policy
- Reporting any suspected misuse or problem to the Headteacher / E-Safety Coordinator for investigation / action / sanction
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- Pupils understand and follow the e-safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- That they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned students / 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.
-

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the schools E-Safety Policy covers their actions out of school, if related to their membership of the school

This policy, supported by the school's Acceptable Use Agreements for staff, governors, visitors and pupils (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Home-School Agreements, and Behaviour/Pupil Discipline (including the Anti-bullying) Policy and PSHE.

SAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive regular information and training on e-Safety issues in the form of memos from the e-Safety co-ordinator.
- New staff receive information on the school's Acceptable Use Policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

EDUCATION AT BREDENBURY PRIMARY SCHOOL

INTERNET USE WILL ENHANCE LEARNING The school's Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- 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 taught how to evaluate Internet content
- We will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- As pupils progress through the school into Key Stage 2 they will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

PUPILS Whilst regulation and technical solutions are very important their use must be balanced by educating pupils take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's provision. Children and young people need the help and support of the school to recognise and avoid e-safety risk and build their resilience.

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

- Key e-safety messages should be reinforced as part of a planned programme
- Pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules of use of ICT systems will be posted in all rooms with computers
- Staff should act as good role models in their use of ICT, the internet and mobile devices

The children will be taught e-safety through a planned programme of age appropriate lessons, assemblies and training provided by CEOP (the Child Exploitation and Online Protection Centre).

Education – Parents/Carers Parents/carers are expected to read the Acceptable Use Policy for pupils with their child.

A guide to e-safety for parents and carers will be circulated. Parents are invited to training provided by CEOP (the Child Exploitation and Online Protection Centre).

Curriculum E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the website the pupil visits

KEY E-SAFETY PRACTICES

Staff, volunteers and governors sign and agree to abide by the school's Acceptable Use Policy.

When using communication technologies the school considers the following as good practice:

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus and Spyware protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority and with the technician attached to our school.
- Network Security is managed under contract to Edutech

Password security

Staff will take steps to maintain password security. These steps should include:

- Keeping their password secure from others. Using a different password for accessing organisational systems to that used for personal (non-organisational) purposes.
- Choosing a password that is difficult to guess, or difficult for others to obtain by watching them login.
- Adding numbers or special characters (e.g. !@£) can help.
- Changing passwords three-monthly.
- Staff/volunteers should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- In addition, when leaving a computer for any length of time, all staff members/volunteers shall log off or lock the computer, using CTRL+ALT+DELETE or other system command.
- Ensuring that there is a limit on the number of consecutive failed log in attempts. (Best practice is between 3 and 5 attempts)
- Restrict concurrent access i.e. a user should not be able to log in at the same time from two different machines, unless a generic or group login is appropriate.

DATA PROTECTION

Data protection regulations must be followed at all times.

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they:

- At all times take care to ensure that safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

AUTHORISATION OF INTERNET ACCESS

The organisation will maintain a current record of all staff/volunteers, children and young people who are granted access to the organisation's electronic communications.

- All staff/volunteers must read and sign the organisation's policies regarding information security and the use of information technology before using the organisation's ICT resource.
- For younger children, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Young people must apply for Internet access individually by agreeing to comply with the Acceptable Use Policy. (See appendix).
- Parents/carers will be asked to sign and return a consent form for children and young people's access.
- Parents/carers will be informed that children and young people will be provided with supervised and unsupervised Internet access, but must comply with the AUP at all times.

FILTERING

Filtering is managed under contract to Edutech:

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled-garden or "allow-list" restricts access to a list of approved sites. Such lists inevitably limit children and young people's access to a narrow range of information.
- Dynamic filtering examines web page content or email for unsuitable words. Filtering of outgoing information such as web searches is also required.
- Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers can be set to reject these pages.
- Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- If adults or children discover unsuitable sites, the Uniform Resource Locator URL* must be reported to the E-safety Co-ordinator for blocking.

* URL stands for **Uniform Resource Locator**. It is the address of a web page. Each page has its own unique web address (URL). This is how your computer locates the web page that you are trying to find. An example of a URL is: <http://funbrain.com/index.html>. 1 Nov 2001

- The school's broadband access will include filtering appropriate to the age and maturity of children and young people.
- The E-safety co-ordinator will ensure that regular half-termly checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the organisation believes is illegal must be reported to the appropriate agencies such as Children's Social Care or CEOP (the Child Exploitation and Online Protection Centre). See Response to Risk Flowchart
- The organisation's access strategy will be designed to suit the age and requirements of the children and young people, with advice from network managers.

E-MAIL SECURITY

- Children and young people may only use approved email accounts.
- Children and young people must immediately tell an adult if they receive offensive email.
- Children and young people must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole-class or group email addresses will be used for communication outside of the school.
- Access in school/organisation to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and should be restricted.
- The forwarding of chain messages is not permitted.
- Schools/organisations may have a dedicated email for reporting well-being and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team/Senior Manager.

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

- Employee/volunteers should only use school/organisation email accounts to communicate with children and young people as approved by the Headteacher.
- Employee/volunteers should not use personal email accounts during school/organisation hours or for professional purposes.

THE MANAGEMENT OF

SOCIAL NETWORKING AND PERSONAL PUBLISHING

- Staff, volunteers and governors will provide good role models by acting in accordance with our Acceptable Use Policy with regard to social networking.
- The school will control access to social media and social networking sites.
- Children will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Children will be advised not to place personal photos on any social network space. They should consider how public the information is, and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the child or his/her location.
- Employee/volunteer official blogs or wikis should be password protected and run from the organisational website with approval from the Headteacher.
- Employee/volunteer will be instructed not to run social network spaces for children use on a personal basis.
- If personal publishing is to be used with children then it must use age-appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by organisational staff.
- Children will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Children will be encouraged to invite known friends only and deny access to others by making profiles private.
- Children and young people are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

THE MANAGEMENT OF LEARNING PLATFORMS
AND VIRTUAL LEARNING ENVIRONMENT (VLES)

- The Headteacher and staff will monitor the usage of the Learning Platforms by children and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Children and staff will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the Learning Platforms.
- All users will be mindful of copyright issues and will only upload appropriate content onto the Learning Platforms.
- When staff, governors and children leave the school their account or rights to specific school areas will be disabled.
- Any concerns with content may be recorded and dealt with in the following ways:
 - a) The user will be asked to remove any material deemed to be inappropriate or offensive.
 - b) The material will be removed by the site administrator if the user does not comply.
 - c) Access to the Learning Platforms for the user may be suspended.
 - d) The user will need to discuss the issues with the E-safety Co-ordinator before reinstatement.
 - e) A pupil's parent/carer may be informed.
- Children and young people may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

ASSESSMENT OF RISKS

- Bredenbury Primary School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer.
- Neither Bredenbury Primary School nor Herefordshire County Council can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will use audit digital technological to establish if the e–safety policy is adequate and that the implementation of the e–safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

ADDRESSING CYBERBULLYING

- Cyberbullying (along with all forms of bullying) will not be tolerated in Bredenbury Primary School.
- Full details are set out in the school policy on anti-bullying and anti-cyber bullying.
- There will be clear procedures in place to support anyone affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying:
- Children and young people, staff/volunteers and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyberbullying may include:
 1. The bully will be asked to remove any material deemed to be inappropriate or offensive.
 2. A service provider may be contacted to remove content.
 3. Internet access may be suspended for the user for a period of time.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

4. Parents/carers may be informed.
5. The Police will be contacted if a criminal offence is suspected.

ADDRESSING SEXTING

'Sexting' is one of a number of 'risk-taking' behaviours associated with the use of digital devices, social media or the internet. It is accepted that young people experiment and challenge boundaries and therefore the risks associated with 'online' activity can never be completely eliminated. However Bredenbury Primary School takes a pro-active approach to help students to understand, assess, manage and avoid the risks associated with 'online activity'. The school recognises its duty of care to its young people who do find themselves involved in such activity as well as its responsibility to report such behaviours where legal or safeguarding boundaries are crossed.

STEPS TO TAKE IN THE CASE OF AN INCIDENT

Step 1 - Disclosure by a student

Sexting disclosures should follow the normal safeguarding practices and protocols. **For further information please read the Safeguarding Policy.**

A student is likely to be very distressed especially if the image has been circulated widely and if they don't know who has shared it, seen it or where it has ended up. They will need pastoral support during the disclosure and after the event. They may even need immediate protection or a referral to police or social services; parents should be informed as soon as possible (police advice permitting).

The following questions will help decide upon the best course of action:

- Is the student disclosing about themselves receiving an image, sending an image or sharing an image?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Are the school child protection and safeguarding policies and practices being followed?
- For this reason a member of the Safeguarding team should be involved as soon as possible.
- How widely has the image been shared and is the device in their possession?
- Is it a school device or a personal device
- Does the student need immediate support and/or protection?

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- Are there other students and/or young people involved?
- Do they know where the image has ended up?

Step 2- Searching a device – what are the rules?

The policy allows for a device to be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography.

When searching a mobile device the following conditions should apply:

- The search is conducted by the Headteacher or a person authorised by them and one other person
- A member of the safeguarding team should normally be present
- The search should normally be conducted by a member of the same gender as the person being searched. However if the image being searched for is likely to be of a different gender to the person 'in possession' then the device should only be viewed by a member of the same gender as the person whose image it is.

If any illegal images of a young person are found the Safeguarding Team will discuss this with the Police. The Association of Chief Police Officers (ACPO) advise that as a general rule it will almost always be proportionate to refer any incident involving 'aggravated' sharing of images to the Police, whereas purely 'experimental' conduct may proportionately dealt with without such referral, most particularly if it involves the young person sharing images of themselves.

'Experimental conduct' commonly refers to that shared between two individuals (e.g. girlfriend and boyfriend) with no intention to publish the images further. Coercion is not a feature of such conduct, neither are requests for images sent from one person to multiple other young persons.

Any conduct involving, or possibly involving, the knowledge or participation of adults should always be referred to the police.

If an 'experimental' incident is not referred to the Police, the reasons for this should be recorded in the school's 'Safeguarding Incidents Log'.

Always put the young person first. Do not search the device if this will cause additional stress to the student/person whose image has been distributed. Instead rely on the description by the young person, secure the advice and contact the Police.

For further information please read the Sexting Policy.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

E-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with under the school's Complaints Procedure.
- Any complaint about staff misuse must be referred to the Headteacher.
- All e-safety complaints and incidents will be recorded by the school — including any actions taken.
- Children and young people and parents/carers will be informed of the complaints procedure.
- Parents/carers, children and young people will work in partnership with the school to resolve issues.
- Discussions shall be held with/between the school, Children's Social Care, Police and Herefordshire Safeguarding Children Board to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

IMPLEMENTATION AND COMPLIANCE

No policy can protect pupils without effective implementation. It is essential that staff remain vigilant in planning and supervising appropriate, educational ICT experiences.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), I Pads, tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.)

LINKS TO FOLLOW FOR MORE INFORMATION/ADVICE

For advice about e-safety please visit:

www.thinkuknow.co.uk website provided by CEOP (the Child Exploitation and Online Protection Centre).

<http://www.saferinternet.org.uk/advice-and-resources/parents>

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

MANAGING THE INTERNET

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the Herefordshire Grid for Learning (HGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

HOW ARE EMERGING TECHNOLOGIES MANAGED?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use Policy.

HOW WILL THE RISKS BE ASSESSED?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor the LEA can accept liability for the material accessed, or any consequences of Internet access.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher and ICT coordinator will ensure that the Internet policy is implemented and compliance with the policy monitored.

INFRASTRUCTURE

Herefordshire Local Authority has a monitoring solution via the Herefordshire Grid for Learning where web-based activity is monitored and recorded.

School internet access is controlled through the LA's web filtering service. For further information relating to filtering please go to

<http://www.thegrid.org.uk/eservices/safety/filtered.shtml>

- Bredenbury Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, I Pads, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

PERSONAL MOBILE DEVICES (INCLUDING PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use and there are designated areas in school that these can be carried and used.
- Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- The school does not allow pupils to bring personal mobile devices to school and is not responsible for the loss, damage or theft of any brought in.
- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING PHONES)

- The sending of inappropriate text messages between any members of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

MANAGING CONTENT

How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Coordinator.
- The School should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
- Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
- Nominated persons (ICT Coordinator) will be responsible for permitting and denying additional websites as requested by colleagues.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

How should website content be managed?

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

COMMUNICATION

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or nationally and international. We recognise that pupils need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve 'working at or greater depth milestone 2', pupils must have experienced sending and receiving emails.

- The school gives all teaching staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- Staff sending emails to external organisations, parents or pupils are advised to cc. the Headteacher.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Children use a class/ group email address.
- **The forwarding of chain letters is not permitted in school.**
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- **Pupils must** immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- **Staff must** inform the eSafety co-ordinators if they receive an offensive e-mail.

On-line communications and social networking

- Safe use of Social Network sites will be taught as part of the computing curriculum.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Staff will be advised not to communicate with pupils or parents on any Social Network site.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites as part of the e safety programme.

Mobile technologies

- Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
- Pupil mobile phones are not permitted within the school.
- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

INTRODUCING THE POLICY TO PUPILS

- Rules for Internet access will be posted in all rooms where computers are used.
- A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
- Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that Internet use will be monitored.

PARENTS AND E-SAFETY

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Website.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This will include demonstrations, practical sessions and suggestions for safe Internet use at home.
- All parents will receive support information as and when available.

STAFF AND THEIR INCLUSION IN THE E-SAFETY POLICY

- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained.
- The school's consequences for Internet and mobile phone / PDA / technology misuse will be made clear so that all teachers are confident to apply this should the situation arise.
- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- Community users of the school's ICT facilities must sign the acceptable user policy before being granted access.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

SAFE USE OF IMAGES

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the pupils device.

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.
- Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- Pupil's names will not be published alongside their image and vice versa unless permission is sought. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

For further information relating to issues associated with School websites and the safe use of images in Herefordshire schools see:

<http://www.thegrid.org.uk/schoolweb/safety/index.shtml>

STORAGE OF IMAGES

- Images/ films of children are stored on the school's network.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network/ Learning Platform.

WEBCAMS

- Webcams in school are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

For further information relating to webcams, please see:

<http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml>

MISUSE AND INFRINGEMENTS

Complaints

How will complaints be handled?

- Complaints relating to e-Safety should be made to the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Incidents will be logged by the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher. Depending on the seriousness of the offence investigation by the Headteacher/ LA / immediate suspension / possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct by the Headteacher.

Cyberbullying

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on Anti-bullying, Anti-cyberbullying and Behaviour.

- There are clear procedures in place to support anyone in the school community affected by cyberbullying.

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

- All incidents of cyberbullying reported to the school will be recorded

EQUAL OPPORTUNITIES

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's eSafety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of eSafety. Internet activities are planned and well managed for these children and young people.

PARENTAL INVOLVEMENT

- Parents / carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-Safety policy in writing.
- Parents / carers are asked to read through and sign *The Acceptable Use Agreement* on behalf of their child, on admission to school.
- Parents / carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to eSafety where appropriate in the form of:
 - Information and celebration evenings
 - Posters
 - Website/ Learning Platform postings
 - Newsletter items
 - School website

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

REVIEW PROCEDURE

- There will be an on-going opportunity for staff to discuss with the Headteacher any issue of e-Safety that concerns them.
- This policy will be reviewed every 12 months and consideration given to the implications for future whole school development planning.
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Responsible Internet Use - e-safety

Rules for Staff and Students

The school computer system provides internet access to students and staff. This Responsible Internet Use statement will help protect students, staff and the school by clearly stating what is acceptable and what is not.

- ✓ Access must only be made via the user's authorised account and password, which must not be given to any other person.
- ✓ School computer and internet use must be appropriate to the student's education or to staff professional activity.
 - *Copyright and intellectual property rights must be respected.*
- ✓ Users are responsible for e-mail they send and for contacts made.
- ✓ E-mail should be written carefully and politely. As messages may be forwarded, e-mail is best regarded as public property.
 - *Anonymous messages and chain letters must not be sent.*
- ✓ **The use of public chat rooms is not allowed.**
- ✓ The school ICT systems may not be used for private purposes, unless the head teacher has given permission for that use.
- ✓ Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- ✓ The security of ICT systems must not be compromised, whether owned by the school or by other organisations or individuals.

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

✓ Irresponsible use may result in the loss of internet access

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

Pupil responsible Internet use

These rules will keep everyone safe and help us be fair to others

- ✓ I will only access the system with the permission of a member of staff and in the presence of an adult;
- ✓ On a network, I will only use my own login and password, which I will keep to myself;
- ✓ I will not access other people's files or folders;
- ✓ I will only use the school computers for school work and homework;
- ✓ I will not bring in USB or DVD's from outside school unless I have been given permission;
- ✓ I will only e-mail people my teacher has approved;
- ✓ The message I send will be polite and responsible;
- ✓ When using the internet I will not give out my home address or telephone number, or arrange to meet someone;
- ✓ I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know;
- ✓ I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself;

Bredenbury Primary School

E-SAFETY POLICY AND PROCEDURE

October 2020

- ✓ I understand that the school may/will check my computer files and may/will monitor the internet sites I visit.
- ✓ I understand that if I deliberately break these rules, I could be stopped from using the internet or computers.

Bredenbury Primary School Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents.

Any concerns or clarification should be discussed with Dawn Wilson headteacher and school eSafety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed '**reasonable**' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Headteacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school agreement and with written consent of the parent, carer or staff member. Images will not be distributed outside

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

the school network without the permission of the parent/ carer, member of staff or Headteacher.

- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety agreement and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Full Name _____ (printed)

Signature _____

Date _____

Job title _____

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

Bredenbury Primary School
Primary Pupil Acceptable Use
Agreement / eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open or delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

Dear Parent/ Carer

ICT including the internet, email and mobile technologies etc... has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page.

If you have any concerns or would like some explanation please contact the headteacher.

.....

Parent/ carer signature

We have discussed this and _____ (child's full name)

agrees to:

- follow the eSafety rules;
- to support the safe use of ICT at Bredenbury Primary School.

Parent/ Carer Signature

Class Date

Parents' consent for Web publication of work and photographs

I agree that, if selected, my son/daughter's work may be published on the school web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Parent/carers signature

Date

Bredenbury Primary School
E-SAFETY POLICY AND PROCEDURE
October 2020

or

Bredenbury Primary School
Internet Agreement

Pupil:

Class:

Pupils agreement

I have read and understood the school rules for responsible Internet use. I will use the computer system and Internet in a responsible way and obey the school rules at all times.

Signed:

Dated:

Please print name:

Parents' consent for Web publication of work and photographs

I agree that, if selected, my son/daughter's work may be published on the school web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed:

Date: