BARROW 1618

A Church of England Free School

Policy

E Safety

Adopted: February 2013

Member of staff responsible: Headteacher

Review Date: Summer term 2019

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 school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Security.

Responsibilities

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. The named online safety co-ordinator in this school is Joe Leppington.
All breaches of this policy must be reported to Joe Leppington
All breaches of this policy that may have put a child at risk must also be reported to the DSL, Joe Leppington
Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

Scope of policy

The policy applies to:

- pupils
- parents/carers
- teaching and support staff
- school governors
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that pupils who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

End to End E-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use

- Safe and secure broadband from the Telford and Wrekin School ICT Team including the effective management of filtering

- National Education Network standards and specifications **Writing and reviewing the e-safety policy** The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection. The school has appointed the Designated Child Protection Coordinator as the e-Safety Coordinator.

- Our e-Safety Policy has been agreed by senior management and approved by governors

- The e-Safety Policy and its implementation will be reviewed annually

Teaching and learning: Why Internet use is important?

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience

- Internet use is a part of the curriculum and a necessary tool for staff and pupils

Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils

- Pupils will be reminded at the beginning of each term and taught where appropriate 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

- Any web-sites that are given out are checked by the teacher beforehand. Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law

- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Policy and Procedure

The school seeks to ensure that internet, mobile and digital technologies are used effectively, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate online behaviour and use of technology outside of school for pupils, parents/carers, staff and governors and all other visitors to the school.

Use of email

Staff and governors should use a school email account for all official communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address. Pupils may only use school approved accounts on the school system and only for educational purposes. Where required parent/carer permission will be obtained for the account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for Data Protection. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

The use of personal email addresses by staff and governors for any official school business is not permitted.

- All members of staff and governors are provided with a specific school email address, to use for all official communication.

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff and pupils and parents.

Staff, governors and pupils should not open emails or attachments from suspect sources and should report their receipt to Joe Leppington

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Data Protection Officer with details of the site/service. If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with pupils/ families.

- When working with pupils searching for images should be done through Google

Safe Search , Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Adult material that breaches the Obscene Publications Act in the UK
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

Storage of Images

Photographs and videos provide valuable evidence of pupils' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See Data Protection policy for greater clarification).

Photographs and images of pupils are only stored on the school's agreed secure networks which include some cloud based services. Rights of access to stored images are restricted to approved staff as determined by Joe Leppington.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with pupils, must only use school equipment to record images of pupils whether on or off site. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of pupils. Under no circumstance does the school allow a member of staff to contact a pupil or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission from Joe Leppington.

Pupils are not allowed to bring personal mobile devices/phones to school unless they have received specific permission from the Head Teacher (Joe Leppington)

The school is not responsible for the loss, damage or theft on school premises of any personal mobile device.

Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant school policy and procedures, such as: Child protection, Data Protection, Acceptable use.

- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
    - Not use personal devices during teaching periods, unless permission has been given by the headteacher, such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the Designated Safeguarding Lead (Joe Leppington)
- Staff will not use personal devices, such as: mobile phones, tablets or cameras:
    - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
    - Directly with pupils, and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches the school policy, action will be taken in line with the school allegations and grievances policy

If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted

Visitors' Use of Personal Devices and Mobile Phones

- Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour, Child protection and Image use.
- The school will ensure appropriate signage and information is displayed/ provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the Designated Safeguarding Lead of any breaches of school policy.

Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with the Acceptable use policy and other relevant policies

Working Offsite

Barrow 1618 CofE Primary Free School takes the security of personal data very seriously. In

certain circumstances staff may need to access personal data when working offsite. When working offsite all staff should ensure that any personal data taken or accessed offsite is kept secure in line with the school's data protection policy.

Managing Internet Access Information system security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with T&W E-mail
- Pupils may only use approved e-mail accounts on the school system. Pupils may not use any instant messenger applications on school systems. At the date of this policy no email accounts are available to pupils
- Pupils must immediately tell an adult if they receive offensive e-mail or messages
- Pupils must not reveal personal details of themselves or others in e-mail or other electronic communication, or arrange to meet anyone without specific permission from an adult
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted
- Email attachments should not be opened unless the author is known

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published
- The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified
- Pupils' full names will not be used anywhere on the website or Blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

- Pupil's work can only be published with the permission of the pupil and parent

Social networking and personal publishing

- The school will block/filter access to social networking sites
- Newsgroups will be blocked unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Incidents of cyber bullying outside school which has an impact within school be recorded and monitored
- Staff use of Social Networking sites iis outlined in the School Social Media Policy

Managing filtering

- The school will work with the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL will be reported to the Network Manager who will record the accident and escalate the concern as appropriate
- The SLT, ICT Technician and Co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- The filtering system will block all sites on the Internet Watch Foundation (IWF)
- Any material the school believes is illegal will be reported to the appropriate agencies such as IWF, Shropshire Police or CEOP

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
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden
- Mobile phones should be handed in to the school office for safekeeping. Their security cannot be guaranteed in any other location. All mobile telephones are brought to school at the owner's risk and the school will not be responsible for their loss, however caused

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998

Policy Decisions Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials

- Parents and children will be asked to sign and return a consent form when joining the school.

- Any person not directly employed by the school will be asked to sign an acceptable ICT use agreement before being allowed to access the internet from the school site

Assessing risks

- 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 Academy Trust can accept liability for the material accessed, or any consequences of Internet access

- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective. The audit will be linked with the review of this policy

Managing the Safety of the School Website

- The school will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE)
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupils' personal information will not be published on our website; the contact details on the website will be the school address, email and telephone number.
- The administrator account for the school website will be secured with an appropriately strong password.
- The school will post appropriate information about safeguarding, including online safety, on the school website for members of the community.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Head Teacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaints procedure
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all classrooms and discussed with the pupils every year.
- Pupils will be informed that network and Internet use will be monitored

Staff and the e-Safety policy

- All staff will be given the school e-Safety Policy and its importance explained
- All staff will sign the School's ICT Acceptable Use Policy
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

Awareness and engagement with parents and carers

- Barrow 1618 CofE Primary Free School recognises that parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies.
- The school will build a partnership approach to online safety with parents and carers by:
    - Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
    - Drawing their attention to the school online safety policy and expectations in newsletters, letters, our prospectus and on our website.
    - Requesting that they read online safety information as part of joining our school, for example, within our home school agreement.

- Requiring them to read the school AUP and discuss its implications with their children.

Approval by Governing Body and Review Date

This Policy has been formally approved and adopted by the Governing Body at a formally convened meeting of the Curriculum Committee with delegated powers

Adopted on: February 2013 by the Curriculum Committee

Member of staff responsible: Headteacher

Review date: Summer 2019