



BARNSOLE PRIMARY TRUST

ICT ACCEPTABLE USE POLICY

Policy reviewed by
Policy date
Next review due

Board of Trustees
May 2018
May 2020

1. Policy Aims

The aims of this Acceptable use Policy are to:

- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school in a safe and controlled manner.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Make staff and pupils aware that Internet use in school is a resource and a privilege. If the terms of this policy are not met, this privilege will be taken away.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.

2. ICT Vision

At Barnsole Primary School we will develop the learning environments to provide a range of ICT opportunities and tools. This will empower our children to make relevant and safe choices and be flexible as they develop their personalised learning, in line with our school's vision.

3. Strategy

3.1 General

- Virus protection software is used and updated on a regular basis.
- The safeguarding team are responsible for the school's e-safety.

3.2 Pupils' Access to the Internet

At Barnsole we use the Medway Council "filtered" Internet Service, which will minimize the chances of pupils encountering undesirable material.

We will allow pupils to use the Internet when there is a responsible adult present to supervise. However it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils, the expectation we have of pupils. The school will have access to pupils' emails and other Internet related files and can check these on a regular basis to ensure expectations of ICT behaviour and etiquette are being met.

3.3 Expectations of Pupils and Staff using the Internet:

- All pupils are expected to read and agree the Internet Agreement.
- We expect all pupils and staff to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils and staff using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils or staff encounter any such material accidentally, they are expected to report it immediately to an adult and they should report this, so that the Service Provider can block further access to the site.

- Pupils are expected not to use any rude language in their email communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in email and are expected to follow them.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it.
- Pupils and Staff should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet. This is to prevent corruption of data and avoid viruses.
- No programs on disc or CD Rom should be brought in by pupils from home for use in school although staff can seek permission from the Computing team or Head of School. This is for both legal and security reasons.
- Homework completed at home may be brought in on a USB memory stick, but this will have to be virus scanned by the Network Manager before use.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils and Staff consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources. They will also come under the general discipline procedures of the school which comprises an escalating set of measures including a withdrawal of privileges.
- Uploading and downloading of non-approved software will not be permitted.

4. School Website

- The school website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of children's work will be decided by a teacher in accordance with the data protection principles
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website without parental permission.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the school website.

5. Personal Devices

Staff and pupils may only use their own technology in school as part of a pre-arranged educational activity, with permission from a member of the Computing team or Head of School. Inappropriate use is in direct breach of the school's acceptable use policy.

6. Sanctions

Persistent Misuse of the internet by pupils will result in reducing access to the Internet. Misuse of other technologies will result in a complete ban and/or confiscation. Both of these actions will take place for a set period of time agreed by the Head of School. Parents will always be notified.

7. Pupil and Staff agreement

All pupils and staff must agree to the Acceptable Use Policy. Those who do not agree may not use the school ICT facilities. Parents will be advised of non-compliant pupils as their education may suffer. Staff who do not agree may be subject to disciplinary procedures depending on their position in the school.

Barnsole Primary Staff Acceptable Use and ICT Agreement

These conditions are designed to: -

- show what you should and should not do.
- develop good practice.
- maintain the system's security and protect it from viruses.
- prevent misuse.
- record your consent to the School monitoring your internet/email usage.

You should read these conditions and you will be expected to sign them prior to being given access to the Internet. If there is anything that you do not understand, you must ask your line manager to explain. If you don't follow these conditions it could lead to disciplinary action.

Conditions for internet and intranet use

- Staff using the World Wide Web are expected not to deliberately seek out offensive materials. Should any staff encounter any such material accidentally, they are expected to report it immediately to a member of the ICT team.

All members of staff **must** use their school email address when conducting professional business. This includes communicating with parents and students.

All staff must use Egress Switch whenever possible both internally and externally when sending sensitive information via email. When it is not possible to use Egress Switch any sensitive information sent by email **must** be done so via a password protected document.

- Staff are expected to avoid the use of rude or explicit language in their email communications and keep all contact professional. Whether you are using school's equipment or your own you must not post any content on social networking sites that could bring the school or its staff into disrepute. You must not post any content which could affect the safety or well-being of staff or pupils
- Staff should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork unless permission has been granted otherwise. Using the internet during break times and lunch times for personal reasons is allowed, however access to websites and facilities will be limited to those deemed acceptable by the Medway Filter used to secure and protect the school network.
- No program files may be downloaded to the computer from the Internet.
- No programs on disc or CD Rom should be brought in from home and loaded onto computers for use in school without prior permission from the Head of School due to licensing restrictions and copywriting laws.
- Staff may use USB memory sticks or portable / external hard drives issued by the school, but these must be encrypted and will have to be virus scanned before use.

Where it is necessary to take data offsite i.e. medical records for school trips or to work at home the Trusts Data Security Procedures (see separate document) **must** be followed. All data relating to staff, students and parents must be kept private and confidential.

- Personal printing is not allowed on our network for cost reasons.
- No personal cameras or videoing equipment should be brought into school to be used by staff without prior permission from the ICT team or head teacher. If such devices are used only school provided memory cards should be used.
- Use of the Internet to propagate or store pornography, material of a sexual or illegal content or any material which could be offensive or lead to accusations of harassment (including jokes), is strictly prohibited. In addition you should not use the Internet to propagate any computer games or other software which could be considered an abuse of the School's time and resources.
- Internet access is provided subject to Medway Council/The Schools IT Security Policy and should not be used for any of the following:
 - Breaking through security controls, whether on schools equipment or on any other computer system
 - Intentionally accessing or transmitting computer viruses and similar software
 - Intentionally accessing or transmitting information about, or software designed for breaking security controls or creating computer viruses
 - Intentionally accessing or transmitting material which is obscene, sexually explicit, pornographic, racist, defamatory, hateful, incites or depicts violence or describes techniques for criminal or terrorist acts or otherwise represents values which are contrary to Council/Schools Policy
 - Political lobbying or private business
 - Any activity which could cause congestion and disruption of networks and systems
- Staff consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to ICT equipment and Internet resources.

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

I have read the Acceptable Use and ICT Agreement and agree to these safety restrictions.

Signed: _____

Name: _____

Primary Pupil Acceptable Use

Pupil ICT Agreement / E-Safety Rules

- I will only use ICT in school for school purposes.
- I will only use my own school e-mail address when e-mailing
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/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 e-Safety.

I understand these e-safety rules and agree to follow them whilst I am at Barnsole School.

Signed: _____

Class: _____

Date: _____