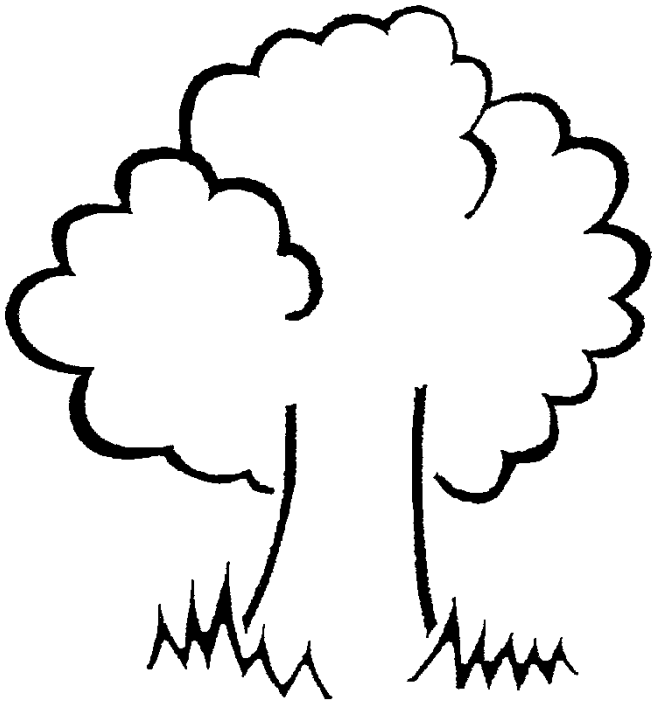
ICT Acceptable Use Policy

2017

Banks Road Infant and Nursery School



Aims of the policy

Banks Road Infant and Nursery School has a duty to provide children and staff with ICT resources and access to the internet as part of their learning experience. The purpose of ICT use in school is to aid raising educational standards, to promote pupil achievement, to give children work/life skills and to support the professional work staff.

The policy is designed to outline the acceptable use of computers including the use of internet and e-mail. It is a dynamic document in that it will respond to the everchanging ICT environment at the school, as we attempt to stay up to date with ICT advancements to support the national curriculum. It will therefore be added to and amended as applicable. It is our aim to highlight the 'personal responsibility' of the computer user, whether it is for drafting class work on a word processor or using the internet or preparing lessons.

This document sits alongside the school e-safety policy which outlines specific information about our responsibility for keeping safe and how we teach children to manage their digital footprint and stay safe when using the internet.

E-Safety – We aim to teach children how to keep themselves safe so that they are prevented from being exploited and free from extremism. We shall do this by teaching skills and through our values and philosophy of work.

Objectives of the policy

1. Allow staff and pupils the chance to access computer equipment, the internet and email, for educational purposes.
2. Set guidelines for acceptable use of the equipment, hardware and software, so staff and pupils are aware of what I acceptable and not acceptable.
3. Protect pupils and staff from undesirable information, particularly on the world wide web (WWW).
4. Provide rules which are consistent, and in agreement with Nottinghamshire County Council.

Expectations of the ICT User

The following guidelines set banks road Infant and nursery School's expectations for the acceptable use of equipment and use of computers generally around the school by staff and pupils. Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to a member of the senior management Team.

Passwords – passwords are the responsibility of the user and in no circumstances, should they be disclosed in any way. If you suspect somebody knows your password then contact the IT system manager as soon as possible.

Unacceptable files – On a regular basis the IT systems manager will search the network for illegal or unacceptable files; which will in turn be removed.

Network etiquette and Privacy

Users are expected to abide by the rules of network etiquette, these rules include, but are not limited to, the following:

- Be polite – never send or encourage others to send abusive messages.
- Use appropriate langue – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other group.
- Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other user's files or folders.
- Password – do not reveal your password to anyone. IF you think someone has learned your password then contact ICT Team.
- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users fining machines logged on under another user's user name should log off the machine whether they intend to use it or not.

Hacking - Hacking into or attempting to corrupt the network settings, software or hardware will not be tolerated. Any attempts to do so will be picked up through regular network checks and will be dealt with by a member of the senior leadership team.

Computer damage – Any incidents of damage to the computers (hardware and software) needs to be reported to the IT systems manager immediately; this will then be followed up accordingly.

Use of the internet and e-mail

Banks road Infant and nursery school uses a filtered, broadband internet service provider for e-mail and internet access. Pupils and staff will be allowed to use the internet to search for information and resources to meet their professional and learning objectives for information in the school. Pupils and staff will need to be aware that there is no regulatory authority body for the internet, anyone, anywhere can publish materials. It is not censored for opinion, bias or validity of information.

Guidance for school staff regarding social networking sites outside of school

For those who belong to a social networking site (eg Facebook, Twitter, My Space) there are some important issues to note if you want to protect yourself.]

- DO not accept any contact with current of previous pupils
- IF under 18s are on your list be especially careful that content is appropriate including photos.
- Avoid bad language, sexual connotations, obscene jokes
- Avoid criticism of your employer
- Do not post photos of colleagues without their prior permission
- Check privacy settings and do not post comments that may bring your professional status and school into disrepute.
- DO not be friends with the parents/carers of children you have met through your work at Banks Road Infant and Nursery School

Remember that these sites are not always private – often there is a wide access. Ensure that your privacy settings are set to private. Do not say anything that you would not say in public or post comments associated with school which could be easily construed as a breach of confidentiality of even bullying. This is especially important as there have been cases across the country where people have be shown to be showing poor judgement in relation to professional conduct and/or safeguarding which may be recorded on their permanent record which could affect references.

Use of Digital Images

For the purposes of this section publication includes on websites, including social media, in the press, on TV, as web broadcasts or video/CD/CDC to be released into the public domain.

Photography using mobile phones

The use of a mobile phone to take pictures in school is prohibited. If photos were taken using a mobile phone in school an allegation could be made that members of staff have taken inappropriate images with those cameras. Staff are strongly advised to bot use the camera within their personally owned mobile phone while on school business. Staff should always use school owned camera and adhere to the schools policy on photography which outlines where Parental permission is required. If a personal phone is used inadvertently and images must be uploaded to the school network at the earliest opportunity and deleted from the phone with no copies having been kept or transmitted elsewhere and the use reported to the SLT.

School Laptops/Netbooks/iPads/Tablets

Staff should ensure that they have absolute control of a school Resources and its use when it is allocated to them. Each member of staff must remember that for a “third party” to use school resources in their home, they would either need to be:

- Logged on by the member of staff personally responsible for the laptop
- Provided with the confidential log in details by the member of staff responsible for the laptop

With this in mind, staff should think about who would be culpable in the unlikely event of an allegation being made.

When persons are viewing material on the internet all people without the assistance of content filters have to make judgements as to whether the content is appropriate or inappropriate. However – inappropriate means different things to different people.

Laptop/Netbook/iPad/Tablet/Learn pad Security

Staff should be aware of the need to preserve the confidentiality of all school information. All personal information is subject to the Data Protection act and should be treated as such.

All staff will be asked to sign a consent form if they are borrowing a school Laptop/Netbook/iPad/Tablet/learnpad (device).

THE POLICY WILL BE REVIEWED ANNUALLY.
DATE OF REVIEW BY GOVERNING BODY: June 2018
This policy was reviewed and ratified by the Pupil and Personnel committee in July 2017. Signed: Chair of Governors_____ Date: _____