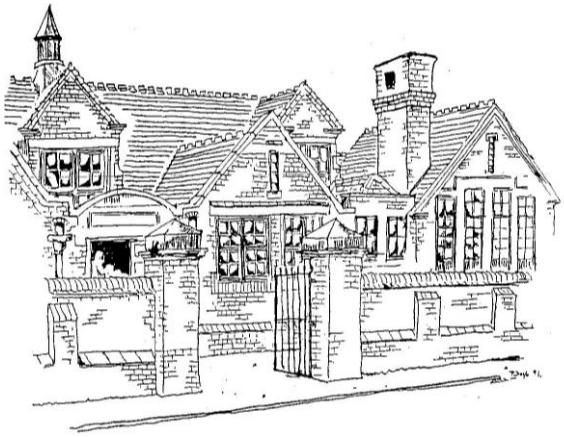
Netherfield Primary School

Acceptable Use Policy

December 2016



Netherfield Primary School Acceptable Use Policy for IT Resources

Context:

This Acceptable Use Policy addresses all rights, privileges and responsibilities associated with Internet use.

The following whole-school policy refers to the safe, acceptable and responsible use of all ICT resources. It is based on local and national guidelines and is incorporated into the school's overall ICT Policy and E-Safety Policy.

All involved parties must read the AUP carefully to ensure that they all fully understand and accept the contents before signing it.

This Acceptable Use Policy has been approved by the Headteacher, SMT and Governors. It will be reviewed annually.

Created by: Vicky Buckland

Date: 5th December 2106

To be revised: 25th July 2017

Contents:

The Netherfield Primary School network and ATOM Internet access has been established for an educational purpose. The term "educational purpose" includes classroom activities, career development, and quality research activities.

Use of Internet facilities

The school Internet service is provided by Virgin Media. Atom and our IT Technician monitors and audits the use of the Internet and reports any potential misuse they identifies.

If inappropriate material is accessed accidentally, users should immediately report this to a member of staff so that this can be taken into account in monitoring.

Policy Objectives

There are three main objectives to this policy

1.1 To ensure that children, staff, equipment and data are adequately protected against any action that could adversely affect the school

1.2 To ensure that users are aware of and fully comply with all relevant legislation

1.3 To create and maintain a level of awareness of the need for ICT security to be an integral part of the day to day operation so that all staff understand the need for ICT security and their own responsibilities in this respect

Using the Internet

The school's Internet access incorporates a software filtering system provided by ATOM. This filtering system aims to achieve the following;

- Only allow access to listed approved and educationally appropriate content.
- The content of web pages or web searches is dynamically filtered for unsuitable words/phrases.
- A rating system is used to rate web pages for inappropriate content and the web browsers are set to reject these pages.

The school will immediately report the details of any inappropriate or illegal Internet material found to ATOM and/or edit school services.

Netherfield Primary School expects all users to use the Internet responsibly and strictly according to the following conditions:

A summary of unacceptable Internet usage

Users shall not use the school Internet* system to:

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

- pornography (*including images, video as well as explicit animation and textual descriptions*)
- promoting discrimination of any kind (*including material that promotes intolerance on the basis of gender or sexual orientation*)
- promoting racial or religious hatred
- promoting illegal acts
- promoting drugs and substance abuse (i*ncluding web sites that promote the use, manufacture and distribution of illegal drugs, as well as sites that promote the abuse of legal substances such as prescription drugs or the sale of alcohol to minors*)
- graphic portrayal of violence, as well as sites that promote violence or self-endangerment, or contain instructions for making weapons of violence or the sale of such weapons
- any other content which may be offensive to pupils or staff

2.2 Access web-based chat sites that allow users to make contact with individuals in the outside world without providing sufficient safeguards and protection to young people

2.3 Access personal web-based email services other than for professional business use

2.4 Access sites offering Internet-based SMS messaging services

2.5 Run any form of private business or create, edit or access your own web pages outside the school network

2.6 Visit sites that might be defamatory or incur liability on the part of the school

2.7 Upload, download, or otherwise transmit (*make, distribute or distribute*) commercial software or any copyrighted materials belonging to third parties outside the school

2.8 Reveal or publicise confidential or proprietary information, which includes but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships

2.9 Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (*sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion*) that substantially hinders others in their use of the Internet

2.10 Solicit, represent personal opinions or reveal confidential information or use it in any other way that could reasonably be considered inappropriate

2.11 Carry out political lobbying, either directly or via email. But users can use the system to communicate with elected representatives and to express your opinion on political issues

(**for the purpose of this policy, Internet usage means any connection to the Internet via Web browsing, FTP, external email or news groups*)

Further guidance on pupil Internet and email access

3.1 All pupil Internet access must be supervised. This means there **must** be a member of staff in the room who is aware that the pupil is accessing the Internet

3.2 Inappropriate Access to online material

- Internet access is filtered through our Internet Service Provider (ISP). This is not infallible but pupils who deliberately try to access filtered material or bypass the filtering service will have their Internet access reviewed and a support plan put in place to ensure 1:1 supervision and scrutiny/monitoring of use or possible suspension

3.3 Misuse of the Internet will result in the review and possible suspension of Internet access for a fixed period of time

3.4 You may not create or edit personal web pages without approval from a member of staff. Any content added using the school Internet access is the responsibility of the school and must therefore be checked and approved by a member of staff. Pupils are requested not to add a guestbook etc. to such sites because of their unregulated nature

3.5 Pupils should not access website guestbooks, forums or chat rooms due to the unregulated nature of the content, unless there is clear educational value and a member of staff is aware of the activity

3.6 Pupils are reminded that any content they upload to the VLE, including their homepages, is visible to all pupils in their year group and all staff

Further guidance on acceptable usage

Users

4.1 Users are those employees, pupils or authorised guests of the school who make use of the ICT systems to support them in their work. All users of the school's systems and data must comply with our requirements for ICT security.

4.2 Users are responsible for notifying the System Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Headteacher and Chair of Governors. If users notice anyone using ICT suspiciously, they have a professional responsibility to report it.

4.3 Users are responsible for the equipment they use, including;

- Physical security of equipment
- Virus updates
- Operating system updates
- Security of data
- Their own passwords

4.4 Users should always sign in using their personal usernames and passwords. They may not sign in using other staff usernames. The only time staff may sign in using a year group login, is when they are working directly with their class or another group of children.

4.5 Once users have finished using school equipment, or if they are leaving equipment unattended, they must 'lock', 'logoff' or 'shut down' their machines. If staff come across a machine that is unattended, they have a professional responsibility to log it off.

4.6 New adult users in school must get permission from the ICT Team, budget manager or Headteacher before accessing the school network.

The following uses of the Netherfield Primary School network are considered unacceptable:

Personal Safety

5.1 Users will not e-mail personal contact information about themselves or other people except for business reasons. Personal contact information includes; your address, telephone, school address, work address, etc.

5.2 Users should not access or contribute to online forums as these are often unregulated.

5.3 Pupil users should promptly disclose to a member of staff or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal Activities

6.1 Users will not attempt to gain unauthorised access to The Netherfield Primary School network or go beyond their authorised access. This includes attempting to log-on through another person's account or access another person's files. These actions are illegal, even if only for the purposes of "browsing".

6.2 Users will not attempt to bypass the ISP filtering system without the specific permission of the ICT Team or Headteacher. Such attempts will result in an investigation which could lead to disciplinary procedures and/or a permanent ban of Internet access.

6.3 Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal and will be reported to the police.

System Security

7.1 Users are responsible for their individual user area and should take all reasonable precautions to prevent others from being able to use it, for example always logging off school computers. Users must not let any other user know their password, unless specific permission has been given by the ICT Team, Headteacher or Business Manager.

7.2 Users will immediately notify the ICT Team, business manager or Headteacher if they have identified a possible security problem. Users MUST NOT go looking for security problems because this will be construed as an illegal attempt to gain access.

7.3 Users will avoid the inadvertent spread of computer viruses. Unchecked USB flash/pen drives must always be virus checked every time they are opened and email attachments that are suspect or from unknown sources should not be opened.

7.4 Users will not download computer programs or files from the Internet without permission from the ICT Team or the Headteacher.

7.5 Users will not try to load computer programs onto the Netherfield Primary School network or attempt to run programs that are not accessed through the Start Menu or Desktop screen.

Inappropriate Language

8.1 Restrictions against inappropriate language apply to public and private email messages, file names, the content of files and material posted on web pages.

8.2 Such inappropriate language includes obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

Email Use

9.1 The school uses an email distribution list to send messages to selected groups of users.

9.2 Users will not email information that could cause damage or a danger of disruption.

9.3 Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by someone to stop sending messages, then they must stop. This must also be reported to the Headteacher.

9.4 Users will not knowingly or recklessly email false or defamatory information about a person or organisation.

9.5 Users will not email chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.

9.6 Children will not use email in lessons without permission from the member of staff taking the lesson. Children will only use school email accounts.

School Website

10.1 An editorial team and IT Technician manages all aspects of placing web pages on the school's website. It has full editorial responsibility and ensures that the content on the site is accurate and appropriate. The website will comply with Education Authority guidelines.

10.2 The copyright of all material produced by the school for display on the school website belongs to the school. Permission to reproduce any other material will be sought and obtained from the copyright owner.

10.3 The contact details for the school will include only the school's postal address, email address, telephone number and fax number. No personal contact information about staff will be published.

10.4 The school will not publish any material produced by students without the agreed permission of their parents. In addition, photographs of students will not be published without a parent or carer's written permission. A student's full name will not be used in association with photographs unless permission has been granted by their parents/carers.

10.5 Website photographs that include students will be carefully selected and will be of a type that doesn't allow individual students to be identified. Group photographs or 'over the shoulder' images are preferred.

Use of resources

11.1 There are only a limited number of computers available during lesson times. Priority will always be given to users who need to use the computers for educational purposes and users must use the Internet only for educational and professional purposes.

11.2 Users will avoid unnecessary printing.

11.3 Accessing and playing unauthorised games via the Internet is not allowed. A limited number of games do have some significant educational value; see the ICT Team for approval.

11.4 Use of non-educational files that reduce the effectiveness and speed of the network must be avoided.

11.5 For copyright reasons, users must not store or download commercial music of video files anywhere on the school network.

11.6 Shared areas on the school network are for transferring files and users are responsible for their removal when they are no longer needed. If users place inappropriate files in a shared area then their network access is liable to be suspended.

11.7 Users must make attempts to conserve resources where available, such as turning projectors off to preserve bulb life.

11.8 Listening to online radio broadcasts or watching website video clips online slows the whole network. Unless this is for educational purposes, and permission has been given by the ICT Team or Headteacher, it is not permitted during lesson times.

Monitoring of the network

12.1 Pupil users should expect only limited privacy in the contents of their personal files on the Netherfield Primary School network.

12.2 Routine maintenance and monitoring of files stored on the Netherfield Primary School network may lead to discovery that users have violated this Policy or the law.

12.3 Routine monitoring of user logs, user files and the screens of pupils using the Internet may lead to discovery that users have violated this Policy or the law.

12.4 An individual search will be conducted if there is reasonable suspicion that users have violated this Policy. The investigation will be reasonable and related to the suspected violation.

12.5 Parents have the right at any time to request to view the contents of pupils' digital work folders.

Passwords

13.1 The level of password control will be defined by the ICT Team, IT Technician, business manager, Headteacher and 'Atom school services' based on the value and sensitivity of the data involved, including the possible use if 'time out' passwords, where a terminal is left unused for a defined period of time.

13.2 Passwords for staff users should be changed Yearly and should not be reused. They should be a minimum of 8 characters, including a mix of letters and numbers.

13.3 Pupil users will use individual passwords for school computers set by the IT Technician.

13.4 Passwords should be memorised, not written down.

13.5 A password must be changed if it is affected by a suspected breach of security or there is a possibility that such a possibility could occur; such as

- when a password holder leaves the school.
- when a password may have become known to a person not entitled to know it.

13.6 Users must not reveal their password to anyone, unless specific permission has been given by the ICT Team, Headteacher or Business Manager. Users who forget their password must request the ICT Team or business manager to issue a new one.

Policy violations

14.1 Netherfield Primary School will co-operate fully with local, or government officials in any investigation related to any illegal activities conducted through the Netherfield Primary School network.

14.2 Misuse of the Internet or network will result in user access to these facilities being suspended. Continued misuse will result in the suspension becoming permanent and possible further disciplinary action.

Personal Responsibility

Pupils and staff users should be aware of the following:

15.1 All user actions on the Netherfield Primary School network are logged continuously. This includes the workstation used, the time logged on for, the websites accessed, what software is used and any printing done.

15.2 These logs can be used to track specific actions by users or workstations at any given time.

15.3 Users are responsible for the contents of their user area. If obscene or inappropriate files are found by routine scans then access will be suspended and parents notified.

15.4 Details and/or printouts of any unacceptable material or Internet access will be posted home to parents/guardians and the access to the Netherfield Primary network reviewed, which could result in suspension of privileges.

15.5 Staff should be aware of the serious implications involved with logging onto a separate wireless network other than their own at home.

Virus Protection

16.1 Teachers who have laptops which are taken away from school and may spend periods of days and/or weeks disconnected from the school's network, must take the necessary steps to ensure anti-virus protection software on their laptop is updated as soon as possible after a period of time off the network.

16.2 The school will ensure that every ICT user is aware that any device in the ICT system with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the ICT Team, who must take appropriate action.

16.3 Any third party not normally connected to the school network must be check by 'edit school systems' for viruses and anti-virus software before being allowed to connect to the school network.

Communicating the AUP

17.1 'Code of Practice' posters will be displayed in each classroom and on laptop storage units. Students will be informed of acceptable use procedures for the school network and Internet systems. Students must sign the relevant agreements before being allowed to access the school network of Internet.

17.2 All staff will be provided with a copy of the school's AUP and the requirements within. Teachers are aware that Internet traffic can be monitored and traced to an individual user. Staff will also sign the relevant part of the AUP.

17.3 Parents' attention will be drawn to the school's AUP and any relevant updates by letter, in the school newsletter and on the school's website.

Loaned equipment

18.1 All school IT equipment is the property of Netherfield Primary School, including laptops issued to staff

18.2 All staff should use and treat school equipment with the utmost care

18.3 All school loan sets (cameras etc) should be signed out by each staff member and recorded with the ICT Team

18.4 The staff member signing out equipment is responsible for the care of and potential replacement of any equipment that is loaned out

18.5 Staff must return equipment complete and in working order to the ICT Team before it is loaned out to other members of staff

18.6 It is the responsibility of the staff member who wishes to loan out school equipment to check if it is all in working order (batteries charged etc)

18.7 Staff will request for equipment sets at reasonable times; i.e. before 8:45am, during lunch time or after school.

Personal equipment

19.1 All personal items belonging to staff must be insured under personal liability insurance and are not covered by the school's business insurance.

19.2 Staff may be required to have access to their mobile phones for specific school purposes such as leading a school trip or for communication purposes whilst not on school premises. However, staff must not access their mobile phones for personal use within contracted hours.

Disciplinary Implications

Breaches of this policy may result in disciplinary action up to and including dismissal. It may also result in prosecutions under the Computer Misuse Act 1990, and may lead to prosecution of the school and the individual(s) concerned and/or civil claims for damages.