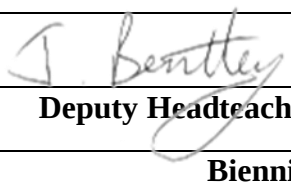
E6

NORTHFIELD SCHOOL ACCESS TO ICT POLICY

Date adopted	**February 17**
Signed by chair of Teaching and Learning committee	
Member of staff responsible for monitoring	**Deputy Headteacher**
Review frequency	**Biennial**

Date	Changes made	Agreed by	Authorised for use by	Date of review

Northfield School ICT/Computing Policy

Introduction

The purpose of ICT use (including the internet) at Northfield School is to help raise educational standards, to promote student achievement, to support the professional work of staff and to enhance Northfield's management of administration systems.

The internet is an essential element in 21st century life for education, business and social interaction. Northfield has a duty to provide students with internet access as part of their learning resources. Internet use is a part of the statutory curriculum and is a necessary tool for staff and students.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

This policy includes details of the school network, acceptable use of the computers and e-safety.

1. The School Network

Northfield school's network is managed by Online PC Support (http://www.onlinepcsupport.co.uk) from their base in Southampton.

All staff can access the academic network from home via remote access, any school workstation or school laptops. Access is via a username and a private password which is given by Online PC Support.

Staff have additional access rights on the system including read/write access to Resources and Staff resources. It is therefore important that passwords are not disclosed or revealed, and that computers are not left logged on or unlocked. Passwords can be changed by contacting Online PC Support if a breach of security is suspected. Staff passwords are changed on a termly basis.

Student data, (for example EHCP documentation, safeguarding and other agency data) is stored securely in separate drives, some of which only senior management have access to.

Broadband internet access is available on all school computers, and all internet content is filtered. All Internet use and emails are monitored and logged. If a website which is blocked is needed for a legitimate reason, for example, a lesson, Online PC Support can temporarily disable the filtering for the website if advised in advance. Primarily, the provision of internet access in school is to facilitate lesson preparation and administrative tasks and should not be used for any other personal tasks or for recreational purposes.

Software installed on the system must be appropriately licensed for the number of machines on which it will be used. Online PC Support will carry out all installations where the software is suitable for the system. Staff must not attempt to install any programs themselves and must respect the licensing laws.

There are 3 ICT suites and 20 laptops that can be booked for groups when they are not being used for ICT/Computing lessons. All bookings must be made through the ICT Suite and Equipment booking forms which are available in each of the ICT rooms, and there is a specific folder for booking out the laptops. Teachers are required to ensure that all computers are logged off at the end of the lesson, chairs are left under tables and that all paper and resources are cleared. It is the responsibility of the teacher to ensure that all equipment and furniture is used following Health and Safety guidelines. The teacher should also ensure that ICT/Computing displays and resources are not tampered with.

Staff are asked to enforce the ***Computer Acceptable Use Policy (annex 1)*** to ensure the safety of the students and the integrity of the network. Unsupervised pupils should not be sent from lessons to the ICT suite to use spare computers without prior arrangement with staff teaching in the ICT suite. The ICT/Computing department will accommodate legitimate requests wherever possible. Most classrooms have a fixed data projector and multimedia centre including a computer. Most rooms also have Interactive Smart Boards for use in lessons and, these should be treated with care as damage can be easily caused. All computer faults and issues should be reported to Online PC Support via email or telephone. Requests for printer cartridges/toner should be ordered using an order form and given to the bursar for purchasing.

All printing should be of a reasonable amount and should not include unnecessary colour prints which reduce the quantity of ink available for legitimate purposes. Large documents should be printed to the photocopier with the colour option selected if necessary.

ICT suites are available throughout the school day for timetabled lessons and instances where staff have booked the rooms for specific lessons. Students must be supervised at all times and should not be left on their own.

General and Best Practice for Staff

- Think before you print. Printing is expensive and consumes resources, which is bad for the environment. Anything that has been printed that is not work related will be confiscated unless it has been authorised by a member of staff.
- Priority must be given to pupils wishing to use the computers for school use.
- Always log off your computer when you have finished using it.
- Storage space on the school network is only for school work.
- Avoid saving or printing huge files (for example, above 15 MB) - if in doubt ask an ICT teacher.
- Manage your files regularly by deleting old items or unneeded items and emptying your recycle bin.
- Leave your computer and the surrounding area clean and tidy.
- If a webpage for which you feel you have a legitimate use is blocked, please speak with an ICT teacher. The web page can be unblocked if approval is given.
- The school's internet connection should be used with consideration for others. Any users found to be using bandwidth inappropriately or unfairly will be excluded from the network.
- Always remember child protection, safeguarding and data protection
- Social media should be used with caution. Staff should ensure they have make appropriate choices to protect your personal life from unwanted attention from pupils, parents and other professionals.

- Do not ‘friend’ or chat with pupils or parents without prior authorisation from a member of the SLT.
- Staff must not take any pupil related data in any form offsite. Access to the school network is available through our secure Virtual Private Network (VPN) or through our web based systems.
- Staff must not use personal IT equipment to record pupil related information (Other than as described above) including the use of a smart phone as a camera.

Internet Filtering Policies

All computers connected to the school’s ICT network infrastructure receive filtered internet access provided by an in-house proxy server managed by Online PC Support. All pupils’ internet access is regulated by a filtering policy. YouTube and other audio-video websites (for example, iPlayer, Channel 4oD, ITV Player, Five Demand) are available to pupils during the school day but staff need to be vigilant of the age appropriateness of videos and audio students can access. Social networking sites (Facebook, Twitter, Instagram and web based email) are all restricted and no access is permitted for students whilst at school. (**See cyber safety policy annex 2**)

Annex 1.

Computer Acceptable Use Policy for Students

The use of technology is actively encouraged at the school, and with this comes a responsibility to protect both pupils and the school from abuse of the system. All pupils, therefore, must be support so that they adhere to the policy set out below. This policy covers all computers, laptops and electronic devices within the school, irrespective of who is the owner. All pupils are expected to act responsibly when using the school computer network, as they would in classrooms and in other areas of the school. The network is monitored and any inappropriate use will be investigated. A breach in compliance might also constitute a breach in law.

General and Best Practice for Students

- Anything that has been printed that is not work related will be taken unless it has been authorised by a member of staff.
- Always log off your computer when you have finished using it.
- Storage space on the school network is only for school work.
- Avoid saving or printing huge files (for example, above 15 MB) - if in doubt ask an ICT teacher.
- Manage your files regularly by deleting old items or unneeded items and emptying your recycle bin.
- Leave your computer and the surrounding area clean and tidy.
- If a webpage for which you feel you have a legitimate use is blocked, please speak with an ICT teacher. The web page can be unblocked if approval is given.
- The school's internet connection should be used with consideration for others. Any users found to be using bandwidth inappropriately or unfairly will be excluded from the network.

Personal Online Safety

- Students should be extremely cautious about revealing personal details and never reveal a home address, phone number or email address to strangers.

- Students should inform a teacher or another member of staff if they have received a message or have visited a website that contains inappropriate language or makes them feel uncomfortable in any way.

- Students should not play with or remove any cables etc that are attached to a school computer.

- Students should be themselves and not pretend to be anyone or anything that they are not on the internet.

- Students should not arrange to meet with anyone they have met on the internet - people are not always who they say they are. If in doubt , students should ask a teacher or another member of staff.

System Security

- Students should not attempt to go beyond their authorised access. This includes attempting to log on as another person, sending email whilst masquerading as another person, or accessing another person's files. They are only permitted to log on using your account details.

- Students should not give out their password to any other pupil. In the event that a pupil uses an account other than their own and is in breach of this policy the account holder and the perpetrator will both be held to account. . If a pupil suspects someone else knows their password, they should let a member of staff know so that Online PC Support can change it.

- Students should not make deliberate attempts to disrupt the computer system or destroy data; e.g. by knowingly spreading a computer virus, altering data or altering global settings.

- Students should not alter school hardware in any way.

- Students should not knowingly break or misuse headphones or any other external devices for example printers, mice.

- Students should not attempt to connect to another pupil's laptop or device while at school. Establishment of your own computer network is not allowed.

- Students should not eat or drink whilst using a computer or in the computer rooms.

Inappropriate Behaviour

Inappropriate behaviour relates to any electronic communication whether email, blogging (for example, online diaries), texting, journal entries or any other type of posting / uploading to the internet.

- Students should not use indecent, obscene, offensive or threatening language.

- Students should not post or send information that could cause damage or disruption.

- Students should not engage in personal, prejudicial or discriminatory attacks.

- Students should not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.

- Students should not knowingly or recklessly send or post false, defamatory or malicious information about a person.

- Students should not post or send private information about another person without them agreeing first.

- Students should not use the internet for gambling.

- Bullying of another person whether by email, online or via texts, will be treated in the same way as any other form of bullying. (See Northfield School Behaviour policy for information on Cyber Bullying)

- Students should not access material that is profane or obscene, or that encourages illegal acts, violence, or discrimination towards other people.

- If students mistakenly access such material, they should inform the teacher or another member of staff immediately, or they will be held responsible.

- If students are planning any activity which might be blocked by the internet filtering policies (for example, research into drugs for a legitimate project), please contact the teacher or head of ICT.

- Students should not attempt to use anonymous proxy sites on the internet.

- Students should not take a photo of another student or member of staff without their permission.

- Students should not play games in the ICT rooms unless a member of staff has given permission.

Plagiarism and Copyright

- Plagiarism is taking the ideas or writing of others and presenting them as your own. Students should not plagiarise work that they find on the internet or anywhere else.

- Students should respect copyright. Breaking copyright law occurs when you reproduce a piece of work that is protected by copyright. If students are unsure whether or not they can use a piece of work, you should request permission from the copyright owner. This includes music files and the copying of CDs etc.

Privacy

- All files and email on the system are the property of the school. As such, System Administrators have the right to access them if required.

- Students should not assume any email sent on the internet is secure.

- All internet browsing on the school system is logged and routinely monitored to ensure the ***Computer Acceptable Use Policy*** has not been broken. Background monitoring notifies System Administrators to any inappropriate internet activity. At any point System Administrators can see what is happening without the user's knowledge.

- Monitored internet data can potentially be disclosed to members of the school's Senior Leadership Team and parents.

- If you are suspected of breaking this Computer Acceptable Use Policy, your own personal laptop / device and mobile phone can be searched by staff with the permission of your parents.

- The school reserves the right randomly to search the internet for inappropriate material posted by pupils and to act upon it.

Software

- Students should not install any software on the school system.

- Students should not attempt to download programs from the internet onto school computers.

- Students should not knowingly install spyware or any sort of hacking software or device.

Annex 2

Cyber-Safety Policy for Students

Introduction

The internet and cyber-space are great ways to connect with people and with the World. They are technologies to enjoy and explore, and are going to play an ever-increasing part in our lives.

As we all know, however, this will involve risks and dangers: we all need to be aware of these and need to acquire and develop the knowledge and skills to reduce and avoid them. We have produced this document as a reminder to us all of some basic cyber-wisdom. These suggestions are based on advice provided by respected sources in the field. If there is anything else that you think should be included then let us know.

Advice for the safe use of the internet:

- Always make up usernames which are not linked to your real name.
- Never agree to meet anyone you have met online unless you are sure they are who they say they are, you have discussed it with your parents and you meet them in a public place in daylight.
- Remember that many people in chatrooms and on social networks are not who they say they are.
- Always avoid posting personal information on websites such as social networking sites and in blogs. Information, such as your real name, address, phone number, email address, school, postcode and photos of you in your school uniform can be used to trace you or use your identity.
- Be careful about putting photos of yourself or friends on websites. Never send photos to someone you have met only online.
- Avoid webcam chats, such as Skype, with people you do not know.
- Do not respond to emails from people you do not know.
- Do not respond to any abusive emails. You may feel that you want to defend yourself; once you engage with the sender, however, the situation may escalate. If you receive any abusive emails, keep them. Create a new folder called “Abuse”, and move the abusive mail into this folder. You do not have to read it. When the time comes to take action, this folder of abusive mail and flame mail can be used as evidence.
- Your passwords are very important; never share them, even with friends. Remember that passwords are more secure if they contain a combination of numbers and letters.
- Learn how to block people on email or websites. If someone sends you inappropriate mail, block them. Ask a teacher for assistance with this.

- Do not be afraid to ask for help. A parent, your Form Tutor, the School Nurse, a School Counsellor or any trusted adult will always try to help you.

- Remember to contact the site administrators if you want something to be removed from a website. It is useful to keep a screen shot in case it happens again.

- Remember, by forwarding an email, photo, video etc you may be making a problem worse. You could be unwittingly involving yourself in bullying. You may even be breaking the law.

Helpful Links

www.childline.org.uk

www.childnet-int.org

www.kidscape.org.uk

www.thinkuknow.co.uk

www.safekids.com

www.bbc.co.uk/cbbc/help/safesurfing

www.bullying.org