Northern Lights
LEARNING TRUST

Acceptable and Responsible Use of Internet Policy

Review Date:	**Autumn 2018**
Next review date:	**Autumn 2019**
Person in charge:	**Chief Executive Officer**
Link Director:	**Chair of Board**

Topic	**Page**
Why write and Internet policy?	3
Why is Internet use important?	4
How does the Internet benefit education?	4
How will Internet use enhance learning?	4
How will pupils learn to evaluate Internet content?	4
How will email be managed?	4
How should website content be managed?	5
What are newsgroups and email lists?	5
Can chat be made safe?	5
How can emerging Internet applications be managed?	5
How will Internet access be authorised?	5
How will the risks be assessed?	6
How will filtering be managed?	6
How will the policy be introduced to pupils?	6
How will staff be consulted?	6
How will IT system security be maintained? 7	
How will complaints regarding Internet use be handled?	7
How will parents' support be enlisted?	8
How is the Internet used across the community?	8
References	9 - 10
Notes on the legal framework	11
Appendixes	12 - 19

Why write an Internet policy?

The Internet is an open communications channel, available to all. Applications such as the Web, e-mail and chat all transmit information over the wires and fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism that would be more restricted elsewhere. Sadly e-mail and chat communication can provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, at Northern Lights Learning Trust we will provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

We will protect our school from possible legal challenge wherever possible. The legal system continues to struggle with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers and to use Internet communication to 'groom' children. However, the possession of other obscene or offensive materials is not clearly covered. The Computer Misuse Act 1990 makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". At Northern Lights Learning Trust we will make it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised". However, we are aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and we will ensure that all reasonable and appropriate steps have been taken to protect pupils.

Staff will be aware of many risks of Internet use and will have opportunities for detailed discussion. Advice and training from advisers or child protection officers will be sought. This policy has involved discussion of relevant stakeholders and is agreed by all.

Northern Lights Learning Trust Acceptable and Responsible Internet Policy has been written by the IT subject leader, IT manager and the Headteacher, building on the Sunderland IT Strategy and government guidance. It has been agreed by the senior management and approved by governors and parents.

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;

- inclusion in government initiatives such as the DfE IT in Schools and the Virtual Teacher Centre (VTC);
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DfE;
- mentoring of pupils and provide peer support for them and teachers.

How will Internet use enhance learning?
The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn to evaluate Internet content?
If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT manager and parents will be informed by letter. We will ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Children will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Training should be available to staff in the evaluation of Web materials and methods of developing pupils' critical attitudes.

How will e-mail be managed?
Pupils may only use approved e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mail. Pupils must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone. Whole-class or group e-mail addresses should be used at Key Stage 2 and below.
Access in school to external personal e-mail accounts may be blocked. Excessive social e-mail use can interfere with learning and may be restricted. 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. Access of Virtual Learning Environments (VLE) email accounts at home lies with parental responsibility. Parents are made aware that children have access and their children should be supervised when using this facility, as with any internet use. When using the VLE, if a child receives an offensive email the IT manager will be able to track who sent the email and when it was sent. The matter will then be referred to the Headteacher. (See appendix *5*) The most severe punishment for pupils misusing this system will be the deactivation of their VLE account.

How should Web site content be managed?

The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published. Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Staff and pupils' full names will not be used anywhere on the Web site, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. The IT manager, in consultation with the Headteacher, will take overall editorial responsibility and ensure that content is accurate and appropriate. The Web site should comply with the school's guidelines for publications. The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

What are newsgroups and e-mail lists?
Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.

Can Chat be made safe?
Pupils will not be allowed access to public or unregulated chat rooms. Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised. A risk assessment will be carried out before pupils are allowed to use a new technology in school.

How can emerging Internet applications be managed?
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. The use of mobile phone and PDA cameras is expressively forbidden in school. Parents, pupils and staff must all refrain from discussing the Academy, uploading photographs of/or related to the Academy on social media websites (including Facebook, Twitter etc.).

How will Internet access be authorised?
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. There will be separate access for students and supply staff. No access will be granted under a lettings agreement. 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 will be informed that pupils will be provided with supervised Internet access (Appendix 2). Key Stage 2 children must apply for Internet access individually by agreeing to abide by the Acceptable and Responsible Internet Use statement. (Appendix 6)

Parents and pupils will be asked to sign and return a consent form.
Please see the sample form later in this document. (Appendix 3)

Pupils will not be issued individual email accounts, unless linked to the VLE, but will be authorised to us a group/class email address under supervision.

How will the risks be assessed?
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 Sunderland LA can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. The Headteacher will ensure that the Internet policy is implemented and compliance with the policy monitored.

How will filtering be managed?
The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the IT manager. The IT manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given later). Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the pupil.

How will the policy be introduced to pupils?
Rules for Internet access (appendix 6) will be posted in all rooms where computers are used and a log-on agreement entered by everyone accessing computers. Pupils will be informed that Internet use will be monitored. Instruction in responsible and safe use should precede Internet access. A module on responsible Internet use will be included in the Personal Development programme covering both school and home use.

How will staff be consulted?
All staff must accept the terms of the 'Responsible Internet Use' (Appendix 7) statement before using any Internet resource in school. All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures will be authorised in writing by the Head Teacher or Assistant Headteacher. The Chair of Governors is authorised to monitor the Headteacher's use of the internet [Regulatory of Investigative Powers Act 2000]. Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required. A copy of the Policy and Procedures will be available during staff induction process.

How will IT system security be maintained?
Local Area Network security issues include:

- The user must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use.
- The workstation should be secure from casual mistakes by the user.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus protection for the whole network must be installed and current.

Wide Area Network (WAN) security issues include:

- All external connections must be assessed for security risks including the wide area network connection and any modems staff may wish to use;

- Firewalls and routers should be configured to prevent unauthorised use of software such as FTP and Telnet at the protocol level;
- Decisions on security made by external agencies such as the LA or ISP must be discussed with schools;
- The IT manager will be responsible for monitoring the above.

The Internet is a connection to the outside world that could compromise system performance or threaten user or system security. The downloading of large files such as video and MP3 can compromise system performance. A wide area network (WAN) connection introduces further risks such as pupils trying to access another school. However it also brings the opportunity for industrial strength security in the form of hardware firewalls and the expertise to design and operate them.

- The school IT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
- The IT manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

How will complaints regarding Internet use be handled?
Responsibility for handling incidents will be delegated to the IT manager in consultation with the Headteacher.
Any complaint about staff misuse must be referred to the Headteacher.
Pupils and parents will be informed of the complaints procedure.
Parents and pupils will need to work in partnership with staff to resolve issues.
There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

- Sanctions available include:
- interview/counselling by IT manager and Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, which could ultimately prevent access to files held on the system, including examination coursework.

How will parents' support be enlisted?
Parents' attention will be drawn to the Acceptable and Responsible Internet Use document in newsletters, the school brochure and on the school Web site.
Internet issues will be handled sensitively to inform parents without undue alarm.
A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).

How is Internet used across the community?
Example of Internet access rules in libraries:
Adult users will need to sign the acceptable use policy.
Parents/carers of children under 16 years of age will be required to sign a responsible use policy on behalf of the child.

References

Particularly for Parents and Children

National Action for Children (NCH)
www.nchafc.org.uk/itok/
Parents Guide on Internet usage

Bullying Online
www.bullying.co.uk
Advice for children, parents and schools

FKBKO - For Kids By Kids Online
www.fkbko.co.uk
Excellent Internet savvy for kids; KS1 to KS3

Parents Information Network (PIN)
www.pin.org.uk
Comprehensive guidelines on Internet safety

Parents Online
www.parentsonline.gov.uk/2003/parents/safety/index.html
Interactive learning and safety advice, excellent presentation for parents.

Kidsmart
www.kidsmart.org.uk
An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know?
www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Family Guide Book (DfE recommended)
www.familyguidebook.com
Information for parents, teachers and pupils

NCH Action for Children
www.nchafc.org.uk
Expert advice for children, young people and parents.

Safekids
www.safekids.com
Family guide to making Internet safe, fun and productive

Particularly for Schools

NAACE / BCS
www.naace.org (publications section)
A guide for schools prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

DfE Superhighway Safety
http://safety.ngfl.gov.uk
Essential reading, both Web site and free information pack. Telephone: 0845 6022260

KS2 Internet Proficiency Scheme
www.becta.org.uk/corporate/corporate.cfm?section=8&id=2758
A Becta, DFE and QCA pack to help teachers educate children on staying safe on the internet

Internet Watch Foundation
www.iwf.org.uk
Invites users to report illegal Web sites

Data Protection
www.informationcommissioner.gov.uk/
New Web site from the Information Commissioner

SunderlandVLE
https://www.vle.sunderlandschools.org
Discussion of the research process and how the Web is best used in projects.

Click Thinking: Scottish Education Department
www.scotland.gov.uk/clickthinking
Comprehensive safety advice

Copyright
www.templetons.com/brad/copymyths.html
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.

Internet Users Guide
www.terena.nl/library/gnrt/
A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web.

Alan November – The Grammar of the Internet
www.edrenplanners.com/infolit/
Article explaining how to evaluate Web sites and information

DotSafe – European Internet Safety Project
http://dotsafe.eun.org/
A comprehensive site with a wide range of ideas and resources.

Notes on the legal framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following application to the head teacher. The Rules for Responsible Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

Data Protection Act 1998 concerns data on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

The Telecommunications Act 1984 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964 defines "obscene" and related offences.

References:

Brief introduction to dangers and legal aspects of the Internet.
www.bbc.co.uk/webwise/basics/user_01.shtml

List of useful law resources; see copyright and Internet sections.
http://link.bubl.ac.uk/law

HMSO: Full text of all UK legislation and purchase of paper copies.
www.legislation.hmso.gov.uk