New Hartley First School

''A very caring and nurturing school in which the well-being of every child is paramount.'
'The quality of education continues to be good.'
Ofsted, June 2016

Internet Usage Policy

Status: **Non-Statutory**

Created/Reviewed **Autumn 2010, 2012, 2013,2015**

Next Review: **Autumn 2017**

Introduction

This document sets out the School policy, which is directly in line with Northumberland Council's policy, towards the use of the Internet.

The purpose of this Policy is to describe the acceptable use of the Council's Internet service and its operation and management.

Any queries arising from this Policy or its implementation can be taken up directly with the Information Security Officer at ITSecurity@northumberland.gov.uk

The Information Security Officer is the Owner of this document and has approved management responsibility for its development, review and evaluation.

Summary of Contents:

1. Scope

1.1 This Policy applies to all elected Members, employees, students, members of the public or any other person operating the Internet service provided by Northumberland County Council or using Council premises for this purpose.

1.2 The policy should be read in conjunction with the Council's Code of Conduct and the ICT & Information Security Policy. These documents are available on the Intranet, or from the Information Security Officer at ITSecurity@northumberland.gov.uk

2. Introduction

2.1 Access to the Internet is provided for business use. Business use is seen as accessing the Internet for information relevant to a User's role, responsibilities and duties, and also where access to the Internet is required in order to provide a service to others as part of their duties.

2.2 The Internet can also be used as a means of ordering and paying for business-related goods in certain circumstances. Users must be obtain advice and guidance from the <Procurement Team.

3. Responsibilities

3.1 Users are responsible for ensuring that their use of the Internet is efficient, effective, ethical and lawful at all times.

3.2 All Users must report any security problems or breaches to their supervisor as soon as possible, for reporting on to the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk

3.3 The Council bears no responsibility for any damage or distress caused to Users by their accessing inappropriate or offensive material.

3.4 Service Heads or appropriate Line Managers are responsible for monitoring Internet use within their own department or service, for which management information can be provided by Information Services.

4. Monitoring Internet Usage

4.1 The Council monitors the use of the Internet for legitimate business reasons, including compliance with this policy.

4.2 Monitoring indicates whether Users are attempting to access unsuitable sites and material, or spending an undue amount of time on inappropriate or non-business related Internet activities.

4.3 The Council reserves the right to retain information that it has gathered on Users' Internet usage for a period of up to two years

4.4 By using the internet, users are deemed to be consenting to the monitoring, recording and auditing of internet use.

5. Shared Computers

5.1 All access to the Internet will be through the use of the User's network login ID and password.

5.2 Users are responsible for all internet activity carried out using their network login ID. Therefore, a user must log off from the machine before moving away.

5.3 Any attempt to logon using another person's ID may be regarded as a disciplinary matter.

6. Internet Usage

6.1 All connection to the Internet and Intranet are approved and under the control of the Information Security Officer. Once a computer's Internet access has been set up any necessary changes to settings must only be made by Information Services staff, or in accordance with their instructions.

6.2 Users must NEVER divulge or share passwords. There are NO exceptions to this, and If a password is disclosed, and therefore compromised, a password reset must be requested from the Information Services Service Desk on (01670 53)3333 Advice on the creation of strong passwords can be found in the ICT & Information Security Policy. Such incidents should also be reported to the Information Security Officer on (01670 53)3309 or at ITSecurity@northumberland.gov.uk

6.3 Monitoring of Internet access takes place automatically and certain sites are blocked from access. If Users find that there is a site that is blocked because of its' content but it is considered to be a legitimate site to visit, the Information Services Service Desk on (01670 53)3333 should be contacted.

6.4 When downloading material from the Internet, all downloaded files must be first saved to the C: drive and virus checked before being opened.

6.5 Downloading of any software is strictly forbidden, unless authorised by the Information Security Officer or his/her nominees. This also applies to shareware that may be free of charge on the internet but could create problems to the Council's network.

6.6 Uploading, downloading or otherwise transmitting commercial software, jokes, games etc outside the Council are strictly prohibited

6.7 Access to newsgroups, forums and similar sites are strictly controlled by the Information Security Officer and requests for access must be submitted on the appropriate online form by a recognised senior officer of the department or service from which the request is made.

6.8 Users are not permitted to use their own software or hardware without the consent of the line manager and the Information Security Officer.

6.9 Website registration, licences and contracts

6.9.1 Many useful sites require registration and Users wishing to register on a website for work purposes are encouraged to do so. However, permission should be sought from an appropriate manager before doing so and if there is any doubt or concern the Information Security Officer should be consulted.

6.9.2 Some websites require the Council to enter into licence or contract terms. The terms should be printed off and sent for approval in advance or e-mailed to the Legal Department before a User agrees to them on the Council's behalf.

Users should always consider whether the information on such sites is from a reputable source and is likely to be accurate and kept up to date, as many such contract terms will exclude liability for the accuracy of free information.

6.10 Copyright of material obtained from the Internet

6.10.1 Unless there is specific approval to the contrary it must be assumed that any material obtained from the Internet is subject to copyright and all Users must ensure that they do not commit any breaches of copyright.

6.10.2 Users must comply with any copyright statement on a website; if there is any doubt as to copyright copies must not be made.

6.10.3 Further advice on the implications of copyright legislation is available from the Legal Department.

7. Acceptable Use of the Internet

7.1 Misuse of the Internet may result in disciplinary action or in exceptional circumstances referral to the Police and/or prosecution. Therefore no attempts must be made to access any inappropriate material. See paragraph 7.2.

7.2 Internet facilities must not be used for:

7.2.1 The creation, downloading, transmission or receiving of any illegal, obscene, indecent, immoral, defamatory or racist images, data or other material, or any data capable of being resolved into obscene or indecent images or material

7.2.2 The creation, downloading, transmission or receiving of material which is designed or likely to cause annoyance, inconvenience or needless anxiety to any other Users

7.2.3 The transmission of material which may infringe the copyright of another person, or material that is protected by trade secret

7.2.4 The transmission of unsolicited commercial or advertising material

7.2.5 The unsolicited sending of inappropriate e-mail to large numbers of people, via Outlook or on the Internet

7.2.6 Deliberate activities which result in the corruption or destruction of other Users' data, violating the privacy of other Users or disrupting the work of other Users

7.2.7 Activities which deny or restrict service to other Users such as the overloading of access links or switching equipment

7.2.8 Activities which compromise, or have the potential to compromise, networked resources, such as the introduction of viruses

8. Personal Use

8.1 Personal access is considered acceptable provided that the use is reasonable, properly sanctioned by appropriate line management and is in the User's own time. Similarly, this kind of use is acceptable for officers who operate Council equipment in their homes.

8.2 Personal use of the Internet must not contravene any specific management instructions or interfere with the performance of duties.

8.3 As with business use, personal use of the internet will be monitored as described at paragraph 4 above.

8.4 As with Email, access to the Internet in connection with secondary business activity is prohibited unless approved as part of any formal Council scheme.

8.5 Council email addresses must not be used when accessing websites for personal use which require registration details for access or for ordering goods or services.

8.6 Users should be aware that Information Services do not provide support for personal use and the Council do not accept any liability for issues arising from personal use.