ICT Mobile phone policy for school employees

Policy agreed by the Governing Body on 12 February 2018

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This eSafety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Head Teacher and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

Policy Purpose

ICT and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

1 PURPOSE

The policy defines and describes the acceptable use of ICT (Information and Communications Technology) and mobile phones for school Employees. Its purpose is to minimise the risk to pupils of inappropriate contact from staff, to protect employees and the school from litigation and to minimise the risk to ICT systems.

2
SCOPE
2.1
This policy deals with the use of ICT facilities at North Ridge and applies to all school employees and other authorised users, e.g. volunteers.
2.2.
Non school staff are subject to the Local Authority's ICT Acceptable Use Policy or their employers Employer's policies.

3 SCHOOL RESPONSIBILITIES

3.1
The Governing Body is responsible for ensuring that its employees act in a lawful manner, making appropriate use of school technologies for approved purposes only.
3.2
The Governing Body is responsible for adopting relevant policies and the Headteacher for ensuring that staff are aware of their contents.
3.3
The Headteacher is responsible for maintaining an inventory of ICT equipment and a list of school laptops and mobile phones and to whom they have been issued.
3.4
If the Headteacher has reason to believe that any ICT equipment has been misused, they will consult The Education Lead Officer at the Local Authority for advice without delay. The Officer will agree with the
Headteacher and Policy and Compliance Manager an appropriate strategy for the investigation of the allegations. Incidents will be investigated in a timely manner in accordance with agreed procedures.
3.5
The Headteacher will make it clear that internal school staff should not carry out any investigations unless they are both qualified and authorised to do so.

4 USER RESPONSIBILITIES

Staff found to be in breach of this policy may be disciplined in accordance with the disciplinary procedure. In certain circumstances, breach of this policy may be considered gross misconduct resulting in termination of employment. Users must report all suspected breaches of this policy to the Headteacher.

4.1 Users and their Line Managers are responsible for ensuring that adequate induction, training and support is undertaken to implement this policy.
4.2 By logging on to ICT systems, users agree to abide by this Acceptable Use policy and other policies that relate to the use of ICT.
4.3 All users are expected to act in a responsible, ethical and lawful manner with the understanding that school electronic and manual information may be accessible to the public under the Freedom of Information Act 2000. Users should uphold privacy and confidentiality in accordance with the Data Protection Act 1998. Care must also be taken not to breach another person's copyright, trademark or design, nor to publish any defamatory content.
4.4 Staff who have been given the use of a school laptop will be expected to sign for its use on receipt. Staff may use school equipment for authorised business use only, except as allowed for in paragraph 5.1.
4.5 Staff must follow authorised procedures when relocating ICT equipment or taking mobile devices offsite.
4.6 No one may use ICT resources in violation of license agreements, copyrights, contracts or national laws, or the Standing Orders, policies, rules or regulations of the school or the Local Authority.
4.7 Users are required to protect their password and not share their account details with others for their use, nor utilise another users' account or misrepresent their

identity for any reason. Users must not under any circumstances reveal their password to anyone else.
4.8 No user shall access (e.g., read, write, modify, delete, copy, move) another user's personal electronic documents (including email) without the owner's permission or as allowed by this policy or by law.
4.9 Users must not load or download software on any device without the authorisation of the Headteacher. Periodic audits of software held on ICT equipment will be undertaken.
4.10 Users must take care to store sensitive information, e.g. pupil data safely and to keep its password protected, on all school systems, including laptops.
4.11 Network connected devices must have school approved anti-virus software installed and activated. Users may not turn off anti-virus software. All users of ICT resources have the responsibility to take precautions to prevent the initial occurrence and subsequent spreading of a computer virus. No one may knowingly create, install, run, or distribute any malicious code (e.g. viruses, Trojans, worms) or another destructive program on any ICT resource.
4.13 No one may knowingly or willingly interfere with the security mechanisms or integrity of ICT resources. No one may use ICT resources to attempt unauthorised use, or interfere with the legitimate use by authorised users, of other computers on internal or external networks. Access to networks will be monitored.
4.14Within the terms of the Data Protection Act 1998, Human Rights Act 1998 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Local Authority or school may record or inspect any information transmitted through or stored in its computers, including email communications and individual login sessions, without notice when:

1. There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
2. An account appears to be engaged in unusual or unusually excessive activity.
3. It is necessary to do so to protect the integrity, security, or functionality of ICT resources or to protect the Local Authority or its partners from liability.
4. Establishing the existence of facts relevant to the business.
5. Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities
6. Preventing or detecting crime
7. Investigating or detecting unauthorised use of ICT facilities
8. Ensuring effective operation of ICT facilities
9. Determining if communications are relevant to the business (for example, in the last resort where an employee is off sick or on holiday and business continuity is threatened)
10. It is otherwise permitted or required by law.

4.15 Do not send private, sensitive or confidential information by unencrypted email –particularly to an external recipient - if accidental disclosure could lead to significant harm or embarrassment. Anonymise personal data where possible e.g. by using initials. Use passwords on sensitive documents that must be sent to external recipients.
4.16 Websites should not be created on school equipment without the written permission of the Headteacher.
4.17 No one may use ICT resources to transmit abusive, threatening, or

harassing material, chain letters, spam, or communications prohibited by law. No one may abuse the policies of any newsgroups, mailing lists, and other public forums through which they participate from a school account.

4.18 The following content should not be created or accessed on ICT equipment at any time:

1. Pornography and “top-shelf” adult content
2. Material that gratuitously displays images of violence, injury or death
3. Material that is likely to lead to the harassment of others
4. Material that promotes intolerance and discrimination on grounds of race, sex,
5. disability, sexual orientation, religion or age
6. Material relating to criminal activity, for example buying and selling illegal drugs
7. Material relating to any other unlawful activity e.g. breach of copyright
8. Material that may generate security risks and encourage computer misuse

4.19 It is possible to access or be directed to unacceptable Internet sites by accident. These can be embarrassing and such sites can be difficult to get out of. If staff have accessed unacceptable content or are in receipt of unacceptable material via email, they should inform the Headteacher. This may avoid problems later should monitoring systems be alerted to the content.

PERSONAL USE & PRIVACY

5.1

In the course of normal operations, ICT resources are to be used for business purposes only. The school permits limited personal use of ICT facilities by authorised users subject to the following limitations:

1. Personal use must be in the user’s own time and must not impact upon work, efficiency or costs.
2. The level of use must be reasonable and not detrimental to the main purpose for which the facilities are provided.
3. Personal use must not be of a commercial or profit-making nature.
4. Personal use must not be of a nature that competes with the business of the school or conflicts with an employee’s obligations.

5.2

Personal use of the Internet must not involve attempting to access the categories of content described in section 4.18 that is normally automatically blocked by web filtering software.

6

MOBILE PHONE COMMUNICATION AND INSTANT MESSAGING

6.1

Staff are advised not to give their home telephone number or their mobile phone number to pupils. Mobile phone communication should be used sparingly and only when deemed necessary.

6.2

Photographs and videos of pupils must not be taken with mobile phones.

6.3

Staff are advised not to make use of pupils’ mobile phone numbers either to make or receive phone calls or to send to or receive from pupils text messages other than for approved school business.

6.4
Staff should only communicate electronically with pupils from school accounts on approved school business, e.g. coursework.
6.5
Staff should not enter into instant messaging communications with pupils.
6.6
Staff should not use mobiles for texting or phone calls during working hours. If there is an emergency and you need to leave your phone on please inform a senior member of staff.

Agreed with the Governors date: Dec 2009 Review Date: 2012

Insert data prot policy – held elsewhere……. Delete this one

Policy Document:
Data Protection Policy

As adopted by the Governors of North Ridge High School.

Date Reviewed by the Governors:9th October 2013

Data Protection Policy

General Statement

North Ridge High School fully endorses and adheres to the principles of data protection as outlined in the Data Protection Acts 1994 and 1998. All staff involved in the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines. Hard paper copies are stored in secure areas of the school.

Enquiries

Information about North Ridge High School Data Protection policy can be obtained from the Business Manager.

Fair Obtaining and Processing

North Ridge High School undertakes to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which data is held, the likely recipients of the data and the data subject's right of access. Information about the use of personal data is printed on the appropriate collection form. If details are given verbally, the person collecting the data will explain the issues before collection of the information.

Terms

Processing	Obtaining, recording or holding the information or data or carrying out a set of operations on the information or data.
Data Subject	Means an individual who is the subject of personal data or the person to whom the data relates.
Personal Data	Means data which relates to a living individual who can be identified. Addresses and telephone numbers are examples
Parent	Refers to the meaning given in the Education Act 1996, and includes any person who has parental responsibility for a child.

Registered Purposes

The Data Protection Act Registration entries for North Ridge High School are available for inspection by appointment with the Business Manager. Explanation of any codes and categories is available from the Business Manager who is the person nominated to deal with data protection issues. Registered purposes covering the data held at the school are listed on the school's registration and data collection documents. Information held for these stated purposes will not be used for any other purpose without the data subjects consent.

Data Integrity

North Ridge High School undertakes to ensure that data integrity is achieved by the following methods;

Data Accuracy

Data will be as accurate and up-to-date as is reasonably possible. If a data subject informs the school of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to any data subjects every twelve months so they can check its accuracy and make any amendments. Where a subject challenges the accuracy of their data, North Ridge High School will immediately mark the record as potentially inaccurate. In cases of dispute, we will attempt to resolve the issue informally, but if this proves impossible, disputes will be referred to the governing body for their judgement. If the dispute cannot be resolved at this stage, either side may see independent arbitration. Until resolved, the information will be marked and both versions will be saved.

Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is held. In order to ensure compliance with this principle, North Ridge High School will check records regularly for missing, irrelevant or seemingly excessive information and may contact the subjects to verify certain items of data. Records are checked for irrelevant data annually and the decisions about what can be deleted is made by the Head Teacher or Business Manager.

Length of Time

Data held about individuals will not be kept longer than necessary for the purposes registered. It is the duty of the Business Manager to ensure that obsolete data are properly erased.

Subject Access

The data Protection Acts extend to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a pupil, the school's policy is that:

- Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.

- Requests from pupils who do not appear to understand the nature of the request will be referred to their parents or carers.

- Request from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

Governors

It is normal practice that Governing Body papers are returned and destroyed at the end of each meeting. A file copy is available in the Business Managers Office.

Processing Subject Access Requests

Requests for access must be made in writing. Learners, parents or staff may ask for a Data Subject Access form, available from the School Office. Completed forms should be submitted to the Business Manager, the data protection officer. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access Log Book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 40 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

Authorised Disclosures

North Ridge High School will, in general, only disclose data about individuals with their consent. However there are circumstances under which North Ridge High School's authorised officer may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Pupil data disclosed to authorised recipients related to education and administration necessary for the school to perform its statutory duties and obligations.

- Pupil data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within the vicinity of the school.

- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.

- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the information outside the school.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who need to know the information in order to do their work. We will not disclose anything on pupil's records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything that suggests that they are, or have been, either the subject of or at risk of child abuse.

A "legal disclosure" is the release of personal information from the computer to someone who requires the information to do his or her job within or for the organisation. Provided that the purpose of that information has been registered.

An "illegal" disclosure is the release of information to someone who does not need it, or has no right to it, or one which falls outside the organisations registered purposes.

Data and Computer Security

North Ridge High school undertakes to ensure security of personal data by the following general methods (precise details cannot be revealed)

Physical Security

Appropriate building security measures are in place. Visitors to the school are required to sign in and out, to wear identification badge whilst in the school and are, where appropriate, accompanied.

Logical Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement. All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Overall security policy for data is determined by the Head teacher and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent – North Ridge High School's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the school should be in the first instance referred to the Business Manager.

Individual members of staff can be personally liable in law under the terms of the Data Protection Acts. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as a disciplinary matter, and serious breaches could lead to dismissal. Further details on any aspect of this policy and its implementation can be obtained from the Business Manager.