ICT and eSafety Policies

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.

Table of Contents

eSafety Policy

Policy agreed by the Governing Body on 12 February 2018

Under the public sector equality duty, all schools/academies must have due regard to the need to eliminate discrimination, harassment and victimisation and any other conduct prohibited by the Equality Act 2010; to advance equality of opportunity between those who share a relevant protected characteristic and those who do not share it and to foster good relations across all protected characteristics. This means schools/academies must take into account equality considerations when policies are being developed, adopted and implemented.

Contents

1. Rationale

1.1 New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

1.2 ICT is an integral part of education in school. The use of these technologies can put young people at risk within and outside the school. This is particularly the case for pupils at North Ridge who are all vulnerable due to their learning disability. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyberbullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

1.3 This eSafety policy is used in conjunction with other school policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1.4 The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The eSafety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Development of this eSafety policy

This eSafety policy has been developed by school and consulted with:

- Staff
- Governors meetings
- Parents group
- Also to be made available on our School website

3. Schedule for the development of this eSafety policy

3.1 Schedule:

This eSafety policy was approved by the Governing Body / Governors Sub Committee on:	February 2018
The implementation of this eSafety policy will be monitored by:	SLT, Lead for ICT
Monitoring will take place at regular intervals:	Every year or sooner if there is a major development/ change in infrastructure or policy
The Governing Body will receive a report on the implementation of the eSafety policy annually (which will include anonymous details of eSafety incidents)	Every year or sooner if there is a major development/ change in infrastructure or policy
The eSafety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to eSafety or incidents that have taken place. The next anticipated review date will be:	January 2019
Should serious eSafety incidents take place, the following external persons / agencies may be informed:	Dataspire, Manchester Safeguarding Children Board, Police

3.2 The school will monitor the impact of this policy using:

- Logs of reported incidents (CPOMS)
- Dataspire monitoring logs
- Annual Survey results from pupils, staff and parents

4. Scope of the eSafety Policy

4.1. This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

4.2. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate eSafety behaviour that take place out of school.

5. Roles and Responsibilities

5.1 Governors

- Governors are responsible for the approval of the eSafety Policy and for reviewing the effectiveness of the policy and will do this through receiving regular information about eSafety incidents and monitoring reports.
- The safeguarding governor will be responsible for monitoring e safety.

5.2 Head Teacher and Senior Leadership Team

- The Head Teacher is responsible for ensuring the safety (including eSafety) of members of the school community, through the day to day responsibility for eSafety
- The Deputy Head Teacher is responsible for ensuring that relevant staff receive suitable CPD to enable them to carry out their eSafety roles and to train other colleagues, as relevant
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff.

5.3 Senior member of staff with responsibility for eSafety

- P.Rogers is responsible for ensuring eSafety is covered in the curriculum, takes day to day responsibility for eSafety issues and has a leading role in establishing and reviewing the school eSafety policies and documents
- Heads of department for the pupils in their department
- Head Teacher/Deputy Head Teacher - Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place.
- Deputy Head Teacher – arranges training and advice for staff
- Head Teacher/ Business Manager - liaises with the Local Authority
- Business Manager/ P.Rogers - liaises with school ICT technical staff and Dataspire
- Receives reports of eSafety incidents and creates a log of incidents to inform future eSafety developments
- Attends/ provides reports for relevant meeting of Governors
- Reports regularly to Senior Leadership Team
- Ensures eSafety incidents are dealt with following school procedures

5.4 Dataspire and technical staff based in School

- Ensure the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Ensure the school meets the eSafety technical requirements required to provide safe access to school users and in any relevant Local Authority eSafety Policy and guidance
- Ensure that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- Ensure that appropriate filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Ensure that Dataspire and other school technical staff keep up to date with eSafety technical information in order to effectively carry out their eSafety role and to inform and update others as relevant
- Ensure that monitoring software / systems are implemented and updated as agreed in school policies

5.5 Teaching and Associate Staff are responsible for ensuring that:

- They have an up to date awareness of eSafety matters and of the current school eSafety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the relevant person as detailed further on in this policy for investigation
- Behave in a professional manner when using ICT resources- personal or professional
- Digital communications with pupils must be on a professional level and only carried out using official school systems
- eSafety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school eSafety and acceptable use policy
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of eSafety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

5.6 Child Protection Team

The lead for Child Protection (Head Teacher/ Deputy Head Teacher and Assistant Head) are trained in eSafety issues and are aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyberbullying

5.7 Pupils

- Where able are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy.
- Where able need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking and use of images and on cyber-bullying.
- Should understand the importance of adopting good eSafety practice when using digital technologies out of school and realise that the school's eSafety Policy covers their actions out of school, if related to their membership of the school.

5.8 Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE.

5.9 Associate Users

Associate users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

6 Policy Statements

6.1 Education – pupils

eSafety education will be provided in the following ways:

- A planned eSafety programme as part of ICT / PHSE will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key eSafety messages will be reinforced as part of a planned programme of assemblies and other pastoral activities
- Pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff will act as good role models in their use of ICT, the internet and mobile devices

6.2 Education - parent and carers

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences.

The school will seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website,
- Parents evenings
- Reference to the external agencies

6.3 Education – Extended Schools

The school will offer regular safety workshops in our parent's group meetings

6.4 Education and Training – Staff

All staff receive eSafety training and understand their responsibilities, as outlined in this policy.

Training is offered as follows:

- A planned programme of formal eSafety training is made available to staff
- eSafety training is included as part of the induction programme

6.5 Training – Governors

Governors take part in eSafety training and awareness sessions

6.6 Technical Infrastructure and equipment, filtering and monitoring

- In collaboration with Dataspire the school is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
- Requests from staff for sites to be removed from the filtered list are considered by Dataspire and referred to the Senior leadership team. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the eSafety group
- An appropriate system is in place for users to report any actual / potential eSafety incident
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- Temporary accounts are in place for the provision of temporary access of “guests” (e.g. trainee teachers, visitors, supply teachers) onto the school system.

6.7 Curriculum

- eSafety is a focus in all areas of the curriculum and staff should reinforce eSafety messages in the use of ICT across the curriculum.
- In lessons where internet use is pre-planned, it is teachers responsibility to check appropriate sites as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

6.8 Use of digital and video images

- The Acceptable Staff Use Policy will be referred to
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In

particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year)
- Pupil's work can only be published with the permission of the student and parents or carers.

6.9 Unsuitable and inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users will not engage in these activities in school or outside school when using school equipment or systems.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Capita and/or the school
- Uploading, downloading or transmitting commercial software of any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial/ personal information, databases, computer/ network access codes and passwords)

- Creating or propagating computer viruses or other harmful files

6.10 Responding to incidents of misuse

All members of the school community are responsible users of ICT, and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/ disciplinary procedures.

Any incidents of misuse must be reported to the Head Teacher immediately

Data Protection and Freedom of Information

Policy agreed by the Governing Body on 12 February 2018

Under the public sector equality duty, all schools/academies must have due regard to the need to eliminate discrimination, harassment and victimisation and any other conduct prohibited by the Equality Act 2010; to advance equality of opportunity between those who share a relevant protected characteristic and those who do not share it and to foster good relations across all protected characteristics. This means schools/academies must take into account equality considerations when policies are being developed, adopted and implemented.

Contents

1. Introduction

1.1 The school collects a large amount of personal data including: pupil records, staff records, names, and addresses of those requesting prospectuses, references, fee collection, as well as the many different types of research data used by the school. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

1.2 Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips (including CCTV) or as sound recordings.

1.3 This policy and procedure explains the duties and responsibilities placed on the school under the legislation relating to data protection issues to ensure that all data is handled and stored securely. The document also explains the processes available to individuals to access information held by the school.

2. Scope

2.1 This policy relates to all employees, volunteers, contractors, pupils and parents. It also explains how members of the public may request information held by the school.

3. Data Protection Act 1998

3.1 The Data Protection Act 1998 describes how organisations must collect, handle, and store personal information. The rules apply regardless of whether the data is stored electronically, on paper or in other formats.

3.2 In accordance with the Act, individuals may make a Subject Access Request (SAR), to see any personal information relating to them held by an organisation.

3.3 To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

3.4 The Data Protection Act1998 is underpinned by eight important principles. These state that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside of the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

3.5 To comply with the Data Protection Act the school must:

- Manage and process personal data properly
- Protect the individuals' right to privacy
- Provide an individual with access to all personal data held on them.

3.6 The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the Data Controller under the Act.

3.7 Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

3.8 Every member of staff that holds personal information has to comply with the Act when managing that information.

3.9 The school is committed to maintaining the eight principles at all times. This means that the school will:

- inform Data Subjects why they need their personal information, how they will use it, and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held

- apply records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to applications for access to personal information known as Subject Access requests in the Data Protection Act
- train all staff so that they are aware of their responsibilities and of the school's relevant policies and procedures

4. Dealing with Subject Access Requests

4.1 Any individual, including members of staff, parents and pupils, has the right of access to information held about them. However with children, this is dependent upon their capacity to understand. As a general rule, a child of 12 or older is expected to be mature enough to understand the request they are making. If the child cannot understand the nature of the request, someone with parental responsibility can ask for the information on the child's behalf.

4.2 Requests for personal information must be made in writing and addressed to the Head Teacher. If the initial request does not clearly identify the information required, then further clarification may be sought from the enquirer.

4.3 The response time for Subject Access requests, once officially received, is 40 days calendar days, irrespective of school holiday periods.

4.4 There are some exemptions to the right to Subject Access data that apply in certain circumstances or to particular types of personal information. The following examples are provided for indicative purposes only and are not intended to be exhaustive:

- Responding to a request may involve providing information relating to another individual (a third party). Third party information is that which identifies another pupil/parent or has been provided by another agency, such as the Police, Local Authority, Health Care Professional, or another school. Before disclosing third party information consent should normally be obtained. There is still however a need to adhere to the 40 day statutory timescale.

- Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

4.5 In certain circumstances it may be appropriate to provide redacted (information edited or removed) to protect the legal rights of named individuals or agencies.

4.6 Therefore all information must be reviewed prior to disclosure. Where there are concerns over the disclosure of information then appropriate professional advice should be sought where necessary.

4.7 Where redaction has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

4.8 Information can be viewed at the school with a member of staff on hand to help and explain matters if requested, or provided at a face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

5. The Education (Pupil Information) (England) Regulations 2005

5.1 The Education (Pupil Information) (England) Regulations 2005 only apply to maintained schools, although academies and free schools may elect to follow the principles of the Regulations.

5.2 The Regulations require schools to make a pupil's educational record available for inspection by the parent, free of charge, within 15 school days of the receipt of a written request from the parent. In addition the parent is entitled to receive an annual report and to discuss the contents of the report with the child's teacher'

6. Dealing with a request in accordance with The Education (Pupil Information) (England) Regulations 2005

6.1 All requests must be made in writing to the Head Teacher.

6.2 The identity of the requestor must be established before the disclosure of any personal information, and checks should also be carried out regarding proof of relationship to the child.

6.3 Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- Credit Card or Mortgage statement

Please note that this list is not intended to be exhaustive.

6.4 The school will make a pupil's educational record available for inspection, free of charge, to a parent / legal guardian within 15 school days of receipt of the parent's written request and will also provide a written copy of the record if requested to do so.

7. The Freedom of Information Act 2000

7.1 The Freedom of Information Act 2000 provides public access to information held by public authorities. It does this in two ways:

- Public authorities are obliged to publish certain information about their activities; and
- Members of the public are entitled to request information from public authorities.

7.2 Recorded information includes printed documents, computer files, letters, emails, photographs, and sound or video recordings.

7.3 The Act does not give people access to their own personal data (information about themselves). If a member of the public wants to see information that a public authority holds about them, they should make a Subject Access Request under the Data Protection Act 1998.

7.4 Anyone can make a freedom of information request – they do not have to be UK citizens, or resident in the UK. Freedom of information requests can also be made by organisations, for example a newspaper, a campaign group, or a company.

7.5 Employees of a public authority can make requests to their own employer, although good internal communications and staff relations will normally avoid the need for this.

7.6 Please note that reference in the Freedom of Information Act 2000 to "public authorities" applies to all publically funded schools and academies.

8. Dealing with a request under the Freedom of Information Act

8.1 Any letter or email to the school asking for information is a request for recorded information under the Act, although it may be more appropriate to deal with routine requests for information in accordance with normal procedures.

8.2 The provisions of the Act need to come into force only if:

- The school cannot provide the requested information straight away; or
- The requester makes it clear they expect a response under the Act.

8.3 For a request to be valid under the Freedom of Information Act it must be in writing (includes email), however requesters do not have to mention the Act or direct their request to a designated member of staff.

8.4 The school has two separate duties when responding to these requests:

- to tell the applicant whether they hold any information falling within the scope of the request;

and

- to provide that information

8.5 In accordance with the Act the school will normally respond to the request within 20 working days.

8.9 The school may refuse to provide information requested under the Act in the following limited circumstances:

- It would cost too much or take too much staff time to deal with the request.
- The request is vexatious.
- The request repeats a previous request from the same person.

8.10 Before refusing to provide any information requested, the school should consult the Information Commissioner's Office website at www.ico.gov.uk for more information.

9. Complaints

9.1 Complaints about the above procedures should be made to the Chair of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaints procedure.

9.2 Complaints which are not appropriate to be dealt with through the school's complaints procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

10. Further Advice and Information

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk

ICT Staff Acceptable Use Policy

Policy agreed by the Governing Body on 12 February 2018

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that the young people receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE, iPads, etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will only use my personal equipment to record these images if It is password protected.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.
- I will only communicate with young people and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- If the data on any device is breached I will report it immediately.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (iPad/ laptop / mobile phone / USB device etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand the importance of regularly backing up my work.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others in line with Data Protection. Where personal data is transferred outside the secure school network, it must be encrypted.

- I understand that data protection policy requires that any staff or young person's data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- It is my responsibility to understand and comply with current copyright legislation.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines

Name: ____

Signed: ____

Date: ____

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

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.

Non-school staff are subject to the Local Authority's ICT Acceptable Use Policy or their employers Employer's policies.

3 School Responsibilities

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.

The Governing Body is responsible for adopting relevant policies and the Head Teacher for ensuring that staff are aware of their contents. 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.

If the Head Teacher 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 Head Teacher 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. The Head Teacher 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 Responsibility

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 Head Teacher.

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.

4.14 Within 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:

- There is reasonable cause to believe the user has violated or is violating this policy, any guidelines or procedures established to implement this policy.
- An account appears to be engaged in unusual or unusually excessive activity.
- 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.
- Establishing the existence of facts relevant to the business.
- Ascertaining or demonstrating standards which ought to be achieved by those using the ICT facilities
- Preventing or detecting crime
- Investigating or detecting unauthorised use of ICT facilities
- Ensuring effective operation of ICT facilities
- 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)
- 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 Head Teacher.

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:

- Pornography and “top-shelf” adult content
- Material that gratuitously displays images of violence, injury or death
- Material that is likely to lead to the harassment of others
- Material that promotes intolerance and discrimination on grounds of race, sex,
- disability, sexual orientation, religion or age
- Material relating to criminal activity, for example buying and selling illegal drugs
- Material relating to any other unlawful activity e.g. breach of copyright
- 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 Head Teacher. This may avoid problems later should monitoring systems be alerted to the content.

5 Personal Use & Privacy

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:

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

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.