Bedlington West End First School – ICT and Computing Acceptable Use Policy For Pupils

This policy is intended to be read and agreed in conjunction with the following policies:

- E-Safety
- Child Protection
- Anti-bullying
- Anti-racism
- Data protection

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies 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 policy outlines our purpose in providing access to the Internet, e-mail and other communication technologies at Bedlington West End First School and explains how the school is seeking to avoid the potential problems that unrestricted access could create.

Internet Access in School

- All staff and any other adults involved in supervising children accessing the Internet, will be provided with the school ICT Acceptable Use Policy, and will have its importance explained to them.

- Our school ICT Acceptable Use Policy for Pupils is available for parents on the school website. Using the Internet to Enhance Learning Access to the Internet is a planned part of the curriculum that will enrich and extend learning activities and is integrated into schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use. Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils:

- access to the Internet may be by teacher demonstration

- pupils may be given a suitable web site to access using a link from their year group links page on the school website or by clicking on a link in a teacher-prepared Word document

- pupils may be provided with lists of relevant and suitable web sites which they may access

- older pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected to observe the Rules of Responsible Internet Use and will be informed that checks can and will be made on files and the sites they access.

Pupils accessing the Internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the Internet once they have been taught the Rules of Responsible Internet Use and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the Internet.

Using Information from the Internet

In order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it:

- pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on television

- teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium)

- when copying materials from the Web, pupils will be taught to observe copyright;

- pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using E-mail

Email is to be solely used for educational purposes within school. Pupils are not permitted to send emails to each other or to staff outside of school hours. Email accounts will be supervised by the lead for Computing.

Maintaining the Security of the School ICT Network

Connection to the Internet significantly increases the risk that a computer or a computer network may be compromised or accessed by unauthorised persons. The ICT co-ordinator will update virus protection regularly, will keep up-to-date with ICT developments and work with the LEA as Internet Service Provider to ensure system security strategies to protect the integrity of the network are reviewed regularly and improved as and when necessary. Users should not expect that files stored on servers or storage media are always private.

Ensuring Internet Access is Appropriate and Safe

The Internet is freely available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher and the school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the Internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- our Internet access is purchased from Northumberland County Council which provides a service designed for pupils including a filtering system intended to prevent access to material inappropriate for children;

- our Rules for Responsible Internet Use are signed by parents and children each year;

* Pupils have their own username and password which must be used to access the internet.

- children using the Internet will normally be working during lesson time and will be supervised by an adult (usually the class teacher) at all times;

- staff will check that the sites pre-selected for pupil use are appropriate to the age of the pupils;

- staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan;

- pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others;

- the ICT co-ordinator will monitor the effectiveness of Internet access strategies;

- the ICT co-ordinator will ensure that occasional checks are made on files to monitor compliance with the school's ICT Acceptable Use Policy; 3

- the headteacher will ensure that the policy is implemented effectively;

- methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in accordance with national guidance and that provided by the LEA.

Generally, the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school nor Northumberland County Council can accept liability for the material accessed, or any consequences of this.

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material, responsibility for handling incidents involving children will be taken by the IT Co-ordinator and the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher.

All the teaching staff will be made aware of the incident if appropriate.

- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.

- If staff or pupils discover unsuitable sites the IT co-ordinator will be informed. The IT co-ordinator will report the URL and content to the ISP and the LEA; if it is thought that the material is illegal, after consultation with the ISP and LEA, the site will be referred to the relevant authorities.

Pupils are expected to play their part in reducing the risk of viewing inappropriate material by obeying the Rules of Responsible Internet Use that have been designed to help protect them from exposure to Internet sites carrying offensive material. If pupils abuse the privileges of access to the Internet or use of e-mail facilities by failing to follow the rules they have been taught or failing to follow the agreed search plan when undertaking their own Internet search, then sanctions consistent with our School Behaviour Policy will be applied. This will involve informing the parents/carers. Access to the Internet may also be denied for a period.

Photographs

Prior permission is sought from all parents regarding the use of images for printed publications, media, website and videos. Staff should check the relevant year group permission list before using images of children.

School Website and Twitter

Our school website and social media page on Twitter is intended to:

- provide accurate, up-to-date information about our school
- enable pupils' achievements to be published for a wide audience including pupils, parents, staff, governors, members of the local community and others
- promote the school.

All classes may provide items for publication on the school website. Class teachers will be responsible for ensuring that the content of the pupils' work is accurate, the quality of presentation is maintained and that photo permission forms are checked before submitting items for publication. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status. The class teacher is responsible for uploading pages to the school website and the lad for computing along with the head teacher will ensure that the links work and are up-to-date, and that the site meets legal requirements.

The point of contact on the website will be the school address and telephone number. We do not publish pupils' full names or identify individuals on our web pages. Home information or individual e-mail identities will not be published.

Internet access and home/school links

Parents will be informed that pupils are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future ICT developments both on the website and by newsletter. Pupils have permission to use their passwords for Mathletics, Spellodrome and School 360 at home, in order to support their learning outside of the classroom.

Cyberbullying

Cyberbullying can be defined as the use of Information and Communications Technology (ICT) deliberately to upset someone else and may involve email, virtual learning environments, chat rooms, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites. Through Computing lessons, assemblies and PSHE, children will be taught the SMART rules:

SAFE - Keep safe by being careful not to give out personal information online.

MEETING - Never agree to meet anyone that you chat to on the internet; they may not be who you think they are. You can't be sure who you're talking to on the Internet.

ACCEPTING - Do not accept unusual e-mails. They may be trying to tempt you into opening them. They could contain viruses that can damage your computer. If this happens to you, tell an adult.

RELIABLE - Information on the internet may not be true – anyone can upload material to the internet. Always double check any information on a more reliable website.

TELL - If anything makes you feel worried tell your parents, teachers or an adult that you trust. They can help you to report it to the right place Or call a helpline like ChildLine on 0800 1111 in confidence.

Implementation and review process

This policy was reviewed as part of the E-safety policy agreed by the Strategic Direction Committee of the Governing Body on 28th November 2018 and implemented on 1st December 2018.

AUP agreement statements were created as an Appendix of the E-safety Policy and will be reviewed with the policy on a bi-annual basis or as required by changes in safeguarding responsibilities.

Date of next review: November 2020

Bedlington West End First School – ICT and Computing Acceptable Use Policy For Staff

This policy is intended to be read and agreed in conjunction with the following policies:

- E-Safety
- Child Protection
- Anti-bullying
- Anti-racism
- Data protection
- Code of Conduct
- Disciplinary procedure
- Social media policy
- Digital imaging and cameras policy

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies 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 policy outlines our purpose in providing access to the Internet, e-mail and other communication technologies at Bedlington West End First School and explains how the school is seeking to avoid the potential problems that unrestricted access could create. It also outlines how pupil data will be stored and the protocol to follow if a data breach occurs.

Staff should be given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role. Staff are encouraged to make use of the resources developed by Childnet (http://www.childnet.com)

It is not the intention of the policy to try to police every social relationship that governors may have with parents and school staff but about reminding individuals of the importance of appropriate boundaries, including through their social media use.

Application

This policy applies to the school governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to in this policy as staff or staff members

The policy applies in respect of all ICT resources and equipment within the school and resources that have been made available to staff for working at home. ICT resources and equipment includes computer resources, use of school internet access and email systems, software (including use of software such as SIMS), school telephones and text systems, cameras and recording equipment, intranet and virtual learning environment and any other electronic or communication equipment used in the course of the employee or volunteer's work.

This policy also provides advice to staff in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of staff working with children and young people.

Access

Server and Internet Access

School staff will be provided with a log on where they are entitled to use the school ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, staff can use any facilities available subject to the facilities not being in use by pupils or other colleagues. Access is provided to enable staff to both perform their role and to enable the wider staff in the school to benefit from such facilities. Staff must log out of their account when the equipment is not being used.

Email access

Where staff have been provided with a school email address to enable them to perform their role effectively, it will not normally be used to communicate with parents and pupils. Where staff are able to access email outside of schools hours, the email facility should not routinely be used to email parents outside of normal school hours.

Software access

Access to certain software packages and systems will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.

Laptops, ipads and home working

Some staff may be provided with a laptops and/ or an ipad for the performance of their role. Where provided, staff must ensure that their school laptop/other equipment is password protected and not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Staff must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection. Staff ipads must be locked away at night if they remain on school premises. If you have been teaching with the ipad sets, they must be stored in in the trolley and locked when not in use. Similarly, the school laptops should remain locked when it is not in use. Ipads will be security marked and managed by a management system to monitor and restrict access to inappropriate sites or material and to restrict downloads from the app store. Laptops will also be security marked and serial numbers/allocation recorded .

Digital Cameras

Where the school provides digital cameras and other recording equipment for educational and school business use and it is used away from the school site, it must be kept secure and safe. Where pictures of pupils are taken, staff must ensure that they ensure consent has been provided by parents, and that the school’s policy in relation to use of pictures, is followed. Images should be downloaded from a camera regularly and cameras should be stored in a locked cupboard overnight.

Mobile phones

Mobile phones are not permitted to be used by staff during lesson time and if they are used during the school day they must not be used in the presence of the pupils. Parents must not use their mobile phones when helping on a trip or visit.

Staff may use, in urgent or emergency situations during off site visits, their personal mobile telephones. Where used in these emergency situations and a cost incurred, the school will provide reimbursement of the cost of any calls made. Should staff need to make contact whilst off site, this should normally be undertaken via the school rather than a direct call from the individual's personal mobile. School staff who have access to colleagues' personal contact details must ensure that they are kept confidential.

The school will ensure that Display Screen Equipment assessments are undertaken in accordance with its Health and Safety Policy.

Communication with parents, pupils and governors

The school communicates with parents and governors through a variety of mechanisms. The points below highlight who is normally authorised to use which systems and can directly communicate without requiring any approval before use or to agree content. School must indicate to staff if any other staff are permitted to make contact using the systems below:

School Telephones – all teachers, administrative staff and staff who have been permitted through their roles in pupil welfare or home/school link staff. Normally teaching assistants and lunchtime supervisory staff would need to seek approval from a class teacher where they feel they need to make a telephone call to a parent.

Text System – Office staff. Where, in exceptional circumstances other staff need to send a text, this is normally approved by a member of the Senior Leadership Team.

Letters – All teachers may send letters home, but they must be approved by the Headteacher before sending. Where office staff send letters home these will normally require approval by the Headteacher.

Email – school email accounts should not routinely be used for communication with parents outside school hours. Email is used as a normal method of communication amongst school governors and where governors are linked in particular areas with members of staff, communication may take place via email.

Under normal circumstances, school staff should not be using any of the methods outlined above to communicate directly with pupils.

Social Media - School staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children. Staff should make appropriate use of the security settings available through social networking sites and ensure that they keep them updated as the sites change their settings. Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal.

Staff should refer to the School Social Media Policy which contains detailed advice on the expectations of staff when using social media.

Unacceptable Use

Appendix 1 provides a list of Do's and Don'ts for school staff to enable them to protect themselves from inappropriate use of ICT resources and equipment. School systems and resources must not be used under any circumstances for the following purposes:

* to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share

* to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others

*to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material

*to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally

*to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils

* to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment

* to collect or store personal information about others without direct reference to The Data Protection Act

* to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project

*to use the school's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school

* to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or ICT lead if applicable.

Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the Headteacher or other member of the senior leadership team. Schools are encouraged to use appropriate blocking software to avoid the potential for this to happen. Reporting to the Headteacher or senior leadership team equally applies where school staff are using school equipment or facilities at home and accidentally access inappropriate sites or material. Genuine mistakes and accidents will not be treated unfairly

Staff are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.

School staff must take account of any advice issued regarding what is permitted in terms of downloading educational and professional material to the school server. Where staff are provided with a memory stick for such activity, it must be encrypted.

All staff must review the appropriateness of the material that they are downloading prior to downloading and are encouraged to do so from known and reputable sites to protect the integrity of the school's systems. Where problems are encountered in downloading material, this should be reported to the school's ICT lead.

Where staff are permitted to work on material at home and bring it in to upload to the school server through their memory pens, they must ensure that they have undertaken appropriate virus checking on their systems. All memory pens used must be encrypted.Where provided, staff should normally use their school issued laptop for such work.

Staff must ensure that they follow appropriate and agreed approval processes before uploading material for use by pupils to the pupil ICT system and/or VLE.

Whilst any members of school staff may be involved in drafting material for the school website, staff must ensure that they follow appropriate and agreed approval processes before uploading material to the website.

The school will nominate staff who are responsible for ensuring that all equipment is regularly updated with new software including virus packages and that licences are maintained on all school based and school issued equipment. Staff must ensure that they notify the nominated staff when reporting any concerns regarding potential viruses, inappropriate software or licences.

Staff must ensure that their use of the school's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, staff must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.

Staff must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

Monitoring

The school uses Northumberland County Council's ICT services and therefore is required to comply with their email, internet and intranet policies.

The school and county council reserve the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

*to ensure that the security of the school and county council's hardware, software, networks and systems are not compromised

* to prevent or detect crime or unauthorised use of the school or county council's hardware, software, networks or systems

*to gain access to communications where necessary where a user is absent from work

Where staff have access to the internet during the course of their work, it is important for them to be aware that the school or county council may track the history of the internet sites that have been visited.

To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the Chair of Governors, after discussions with relevant staff in Northumberland County Council's HR, IT and Audit Services and following an assessment to determine whether access or interception is justified.

Whistleblowing and cyberbullying

Staff who have concerns about any abuse or inappropriate use of ICT resources, virtual learning environments, camera/recording equipment, telephony, social networking sites, email or internet facilities or inappropriate communications, whether by pupils or colleagues, should alert the Headteacher to such abuse.

Where a concern relates to the Headteacher, this should be disclosed to the Chair of Governors. If any matter concerns child safety, it should also be reported to the Designated Safeguarding Lead (DSL).

It is recognised that increased use of ICT has led to cyberbullying and/or concerns regarding e-safety of school staff. Staff are strongly advised to notify their Headteacher where they are subject to such circumstances. Advice can also be sought from professional associations and trade unions.

Implementation and review process

This policy was reviewed as part of the E-safety policy agreed by the Strategic Direction Committee of the Governing Body on 28th November 2018 and implemented on 1st December 2018.

AUP agreement statements were created as an Appendix of the E-safety Policy and will be reviewed with the policy on a bi-annual basis or as required by changes in safeguarding responsibilities.

Date of next review: November 2020

Dos and Don’ts: Advice for Staff Appendix 1

Whilst the wide range of ICT systems and resources available to staff, both in school and outside of school, have irrefutable advantages, there are also potential risks that staff must be aware of. Ultimately if staff use ICT resources inappropriately, this may become a matter for a police or social care investigation and/or a disciplinary issue which could lead to their dismissal. Staff should also be aware that this extends to inappropriate use of ICT outside of school.

This Dos and Don’ts list has been written as a guidance document. Whilst it is not fully comprehensive of every circumstance that may arise, it indicates the types of behaviours and actions that staff should not display or undertake as well as those that they should in order to protect themselves from risk.

General issues

Do

• ensure that you do not breach any restrictions that there may be on your use of school resources, systems or resources

• ensure that where a password is required for access to a system, that it is not inappropriately disclosed • respect copyright and intellectual property rights

• ensure that you have approval for any personal use of the school’s ICT resources and facilities

• be aware that the school’s systems will be monitored and recorded to ensure policy compliance

• ensure you comply with the requirements of the Data Protection Act when using personal data

• seek approval before taking personal data off of the school site

• ensure personal data is stored safely and securely whether kept on site, taken off site or accessed remotely

• report any suspected misuse or concerns that you have regarding the school’s systems, resources and equipment to the Headteacher or designated manager and/or Designated Safeguarding Lead (DSL) as appropriate

• be aware that a breach of your school’s Acceptable Use Policy will be a disciplinary matter and in some cases, may lead to dismissal

• ensure that any equipment provided for use at home is not accessed by anyone not approved to use it

• ensure that you have received adequate training in ICT

• ensure that your use of ICT bears due regard to your personal health and safety and that of others

Don’t

• access or use any systems, resources or equipment without being sure that you have permission to do so

• access or use any systems or resources or equipment for any purpose that you don’t have permission to use the system, resources or equipment for

• compromise any confidentiality requirements in relation to material and resources accessed through ICT systems

- use systems, resources or equipment for personal use without having approval to do so
- use other people's log on and password details to access school systems and resources
- download, upload or install any hardware or software without approval
- use unsecure removable storage devices to store personal data
- use school systems for personal financial gain, gambling, political activity or advertising
- communicate with parents and pupils outside normal working hours unless absolutely necessary

Use of telephones, mobile telephones and instant messaging

Do

- ensure that your communications are compatible with your professional role
- ensure that you comply with your school's policy on use of personal mobile telephones

Don't

- send messages that could be misinterpreted or misunderstood
- excessively use the school's telephone system for personal calls
- use personal or school mobile telephones when driving
- use the camera function on personal or school mobile telephones to take images of colleagues, pupils or of the school

Use of cameras and recording equipment

Do

- ensure that material recorded is for educational purposes only
- ensure that where recording equipment is to be used, approval has been given to do so
- ensure that material recorded is stored appropriately and destroyed in accordance with the school's policy
- ensure that parental consent has been given before you take pictures of school pupils

Don't

- bring personal recording equipment into school without the prior approval of the Headteacher
- inappropriately access, view, share or use material recorded other than for the purposes for which it has been recorded
- put material onto the VLE, school intranet or intranet without prior agreement from a member of senior staff

Use of email, the internet and VLEs

Do

• alert your Headteacher or designated manager if you receive inappropriate content via email

• be aware that the school's email system will be monitored and recorded to ensure policy compliance • ensure that your email communications are compatible with your professional role

• give full consideration as to whether it is appropriate to communicate with pupils or parents via email, or whether another communication mechanism (which may be more secure and where messages are less open to misinterpretation) is more appropriate

• be aware that the school may intercept emails where it believes that there is inappropriate use

• seek support to block spam

• alert your Headteacher or designated manager if you accidentally access a website with inappropriate content

• be aware that a website log is recorded by the school and will be monitored to ensure policy compliance

• answer email messages from pupils and parents within your directed time

• mark personal emails by typing 'Personal/Private' within the subject header line

<u>Don't</u>

• send via email or download from email, any inappropriate content

• send messages that could be misinterpreted or misunderstood • use personal email addresses to communicate with pupils or parents

• send messages in the heat of the moment

• send messages that may be construed as defamatory, discriminatory, derogatory, offensive or rude

• use email systems to communicate with parents or pupils unless approved to do so

• download attachments from emails without being sure of the security and content of the attachment

• forward email messages without the sender's consent unless the matter relates to a safeguarding concern or other serious matter which must be brought to a senior manager's attention

• access or download inappropriate content (material which is illegal, obscene, libellous, offensive or threatening) from the internet or upload such content to the school or HCC intranet

• upload any material onto the school website that doesn't meet style requirements and without approval

<u>Use of social networking sites</u>

<u>Do</u>

• ensure that you understand how any site you use operates and therefore the risks associated with using the site

• familiarise yourself with the processes for reporting misuse of the site

• consider carefully who you accept as friends on a social networking site

- exercise caution when accepting friendship requests from parents - – you may be giving them access to personal information, and allowing them to contact you inappropriately

- report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site

- take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain

- ask yourself about whether you would feel comfortable about a current or prospective employer, colleague, pupil or parent viewing the content of your page

- follow school procedures for contacting parents and/or pupils

- through your teaching, alert pupils to the risk of potential misuse of social networking sites (where employed in a teaching role)

Don’t

- spend excessive time utilising social networking sites while at work

- accept friendship requests from pupils

- put information or images on line or share them with colleagues, pupils, or parents (either on or off site) when the nature of the material may be controversial

- post anything that may be interpreted as slanderous towards colleagues, pupils or parents

- use social networking sites to contact parents and/or pupils Cyber-bullying:

Practical Advice for School staff

The development of new technologies and systems e.g. mobile phones, email and social networking websites means that bullying is often now taking on a new form; cyber-bullying. Victims of cyber-bullying can experience pain and anxiety as much as traditional forms of bullying, particularly as it can occur outside of the school and school hours, significantly intruding into the personal life of the victim. Whilst it is difficult for schools and teachers to deal with this as they have no direct control over external websites there are a range of actions that school staff can take to reduce the chances of cyber-bullying occurring and actions that can be undertaken where it has already occurred. The guidelines for Headteachers and Governors in dealing with allegations of bullying or harassment define cyberbullying as “the use of information and communication technologies to threaten, harass, humiliate, defame or impersonate”. Cyberbullying may involve email, virtual learning environments, chat room, social networking sites, mobile and landline telephones, digital camera images and game and virtual world sites. This practical advice supplements the guidelines and provides links to other guidance available to school staff in relation to

Cyberbullying.

DOs

- Keep passwords confidential

- Ensure you familiarise yourself with your school’s policy for acceptable use of technology, the internet and email

- Ensure any social site you use has restricted access

- Ensure that you understand how any site you use operates and therefore the risks associated with using the site

- Consider carefully who you accept as friends on a social networking site

- Report to your Headteacher any incidents where a pupil has sought to become your friend through a social networking site

- Check what images and information is held about you online but undertaking periodic searches of social networking sites and using internet search engines

- Take care when publishing information about yourself and images of yourself on line – assume that anything you release will end up in the public domain

- Be aware that any off-duty inappropriate conduct, including publication of inappropriate images and material and inappropriate use of technology could lead to disciplinary action within your employment

- Liaise with your Headteacher and Head/Leader of ICT to remove inappropriate material if it appears on the school website

- Take screen prints and retain text messages, emails or voice mail messages as evidence

- Follow school policies and procedures for e-safety, including access to and use of email, and the internet

- Follow school procedures for contacting parents and/or pupils

- Only contact pupils and/or parents via school based computer systems

- Keep your mobile phone secure at all times

- Answer your mobile telephone with 'Hello' rather than your name, if the number on the display is unknown to you

- Use a school mobile phone where contact with parents and/or pupils has to be made via a mobile (eg during an educational visit off site)

- Erase any parent or pupil data that is stored on a school mobile phone after use

- Seek support from your manager, professional association/trade union, friend, employee support line as necessary

- Report all incidents of cyberbullying arising out of your employment to your Headteacher

- Report any specific incident on a Violent Incident Report (VIR) form as appropriate

- Provide a copy of the evidence with your Headteacher when you report it and further evidence if further incidents arise

- Seek to have offensive online material removed through contact with the site

- Report any threatening or intimidating behaviour to the police for them to investigate

- Access and use the DCSF guidance on Cyberbullying, specifically the advice on reporting abuse and removal of material/blocking the bully's number/email (see attachment/link below)

- Support colleagues who are subject to cyberbullying

DON'Ts

- Allow any cyberbullying to continue by ignoring it and hoping it will go away

- Seek to return emails, telephone calls or messages or retaliate personally to the bullying

- Put information or images on-line, take information into school, or share them with colleagues, pupils or parents (either on site or off site) when the nature of the material may be controversial

- Accept friendship requests from pupils or parents

- Release your private e-mail address, private phone number or social networking site details to pupils and parents

- Use your mobile phone or personal e-mail address to contact parents and/or pupils

- Release electronically any personal information about pupils except when reporting to parents

- Pretend to be someone else when using electronic communication

- Take pictures of pupils with school equipment without getting parental permission or without being directed to undertake such activity for an appropriate specified purpose

- Take pictures of pupils on your own equipment Childnet International have produced a document, "Cyberbullying: Supporting School Staff" which is a useful source of reference to all school staff and leaders. This is available at http://www.childnet.com/ufiles/cyberbullying_teachers.pdf Further guidance is available to schools in relation to Cyberbullying as a whole school community and specifically

Appendix 2

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	*						*	
Use of mobile phones in lessons				*				*
Use of mobile phones in social time		*						*
Bluetooth enabled				*				*
Taking photos on mobile phones				*				*
Taking photos on digital cameras	*						*	
Use of personal hand held devices eg PDAs, PSPs		*						*
Use of personal email addresses in school, or on school network				*				*
Use of school email for personal emails				*				*
Use of chat rooms / facilities				*				*
Use of instant messaging				*				*
Use of social networking sites			*					*
Use of blogs		*					*	

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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, eg 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 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 NCC and the school					*	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					*	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					*	
Creating or propagating computer viruses or other harmful files					*	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					*	
On-line gaming (educational)			*			
On-line gaming (non educational)			*			
On-line gambling					*	
On-line shopping / commerce			*			
File sharing			*			
Use of social networking sites			*			
Use of video broadcasting eg Youtube			*			

Actions and Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		*	*	*				
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	*	*			*	*		
Unauthorised downloading or uploading of files	*	*			*	*		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person’s account	*	*			*	*		*
Careless use of personal data eg holding or transferring data in an insecure manner	*	*			*	*		
Deliberate actions to breach data protection or network security rules	*	*	*		*	*		*
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	*	*	*		*	*		*
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	*	*	*			*		*
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	*	*	*		*	*	*	*
Actions which could compromise the staff member’s professional standing	*	*				*		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	*	*	*			*		*
Using proxy sites or other means to subvert the school’s filtering system	*	*			*	*		*
Accidentally accessing offensive or pornographic material and failing to report the incident	*	*	*		*	*		*
Deliberately accessing or trying to access offensive or pornographic material	*	*	*		*	*	*	*
Breaching copyright or licensing regulations	*	*	*		*	*		*
Continued infringements of the above, following previous warnings or sanctions	*	*	*		*	*	*	*