Biddick Hall Junior School

e-Safety / Acceptable Use Policy

Written: January 2019
To be reviewed: January 2020
ICT coordinator: C.Lynn
System Manager: ICT Technician Mark Tulip
e-Safety team: M. Collinson, C.Lynn, J. O’Neill, Mark Tulip

1. Content

1. Context

1.1 Development of this Policy

Our school uses Durham County Council Service to access the broadband internet. We are required to comply with Durham County Council's Acceptable Use Policy (AUP) which must be signed and agreed by the Head Teacher.

Our e-Safety/Acceptable Use Policy has been written by the school, building on the guidance provided by ICT in Schools South Tyneside. It will be reviewed annually.

1.2 Aims

This policy is intended to help provide clarification on unacceptable behaviours, relating to any information and communications technology (ICT) owned by Biddick Hall Junior school, or personal technology used within the context of the school (this includes off site visits, using school systems at home etc).

It aims to cover all ICT including:-

- the use of computers on the school network.
- network and internet connectivity.
- all mobile devices including laptops, mobile phones, desktop computers and audio/visual equipment.
- all software, electronic communication and storage systems.

It applies to :-

- staff (teaching and non teaching).
- pupils.
- governors.
- parent helpers.
- visitors.
- community users.

1.3 Teaching and Learning

1.3.1 Benefits of Information and Communications Technology

- The Internet and other digital technologies are an essential element in 21st century life for education, business and social interaction. Biddick Hall Junior School has a duty to embrace such technologies and provide pupils with quality access and guidance, as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning so the school access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Internal networks and electronic communications, portable storage devices, audio visual equipment, laptops and PCs have become an essential part of the educational environment, so the whole school community needs to understand the appropriate and effective use of such technologies, to support teaching and learning.

1.3.2 Risks associated with Information and Communications Technology

There are unfortunately some risks associated with the positive educational and social benefits of using the internet and other digital technologies. Pupils will therefore be:-
• taught what Internet use is acceptable.
• be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
• taught what is not acceptable and be given clear objectives and guidelines for the use of the internet and other digital technologies.

1.4 The Legislation

1.4.1 Background

The responsibilities referred to in the previous sections recognise the requirements of the current legislation relating to the use of ICT systems, which comprise principally of:-
Data Protection Acts 1984, 1998 and 2018 (all as amended);
Computer Misuse Act 1990 (as amended);
Copyright, Designs and Patents Act 1988 (as amended)
The Telecommunications Act 1984 and 2000 (as amended)
The Malicious Communications Act 1988 (as amended)
The Digital Economy Act 2017 (as amended)
• It is important that all staff are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action.
• The general requirements arising from these acts are described below.

1.4.2 Data Protection Acts 1984, 1998 & 2018

• The Data Protection Act exists to regulate the use of computerised information about living individuals. To be able to meet the requirements of the Act, the Headteacher is required to compile a census of data giving details and usage of all relevant personal data held on computer within the school and file a registration with the Information Commissioners Office (ICO). It is important that amendments are submitted where the scope of the system extends to new areas of operation. The 1998 and 2018 Act are consistent with the principles established in the 1984 Act, but extends the regulation to certain manual records as well as computerized information and GDPR.
• It is important that all users of personal data are aware of, and are reminded periodically of, the requirements of the act and, in particular, the limitations on the storage and disclosure of information.
• Failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the ICO.

1.4.3 Computer Misuse Act 1990

Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:-
Unauthorised access to a computer system or data;
Unauthorised access preparatory to another criminal action;
Unauthorised modification of a computer system or data.
• All users must be given written notice that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written ‘inhouse’, will be regarded as a breach of school policy and may be treated as

gross misconduct and that in some circumstances such a breach may also be a criminal offence.

1.4.4 Copyright, Designs and Patents Act 1988

- The Copyright, Designs and Patents Act 1988 provides the legal basis for the protection of intellectual property which includes literary, dramatic, musical and artistic works. The definition of "literary work" covers computer programs and data.
- Where computer programs and data are obtained from an external source they remain the property of the originator. Our permission to use the programs or data will be governed by a formal agreement such as a contract or licence.
- All copying of software is forbidden by the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence or contract.
- The ICT co-ordinator/technician is responsible for compiling and maintaining an inventory of all software held by the school and for checking it at least annually to ensure that software licences accord with installations.
- All users must be given written notice that failure to comply with the provisions of the Act will be regarded as a breach of school policy and may be treated as gross misconduct and may also result in civil or criminal proceedings being taken.

1.4.5 The Telecommunications Act 1984 and 2000

- The Telecommunications Act 1984, section 43 makes it an offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'.
- The Telecommunications Regulations 2000 impose restrictions on the interception of communications such as e-mail.

1.4.6 The Malicious Communications Act 1988

The Malicious Communications Act makes provision for the punishment of persons who send or deliver letters or other articles for the purpose of causing distress or anxiety.

1.4.7 The Digital Economy Act 2017 (as amended)

The Digital Economy Act makes provision including that about electronic communications infrastructure and services; to provide for restricting access to online pornography; to make provision about protection of intellectual property in connection with electronic communications; to make provision about data-sharing; to make provision about internet filters.

2. Managing the School Network and Internet Access

2.1 System security, filtering and monitoring.

2.1.1 Managing the system

- School ICT systems security will be reviewed regularly.
- The e-Safety Co-ordinator is responsible for ensuring that the policy is implemented, updated and complied with.
- The e-Safety Co-ordinator will ensure that the school community is kept up to date with safety issues and guidance in collaboration with the Local Authority and Child Protection authorities.

• Security strategies will be discussed with the Local Authority.
• The school will work in partnership with South Tyneside LA, and Durham County Council to ensure that filtering systems are effective as possible.
• Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
• If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.
• The e-Safety coordinator will ensure adequate procedures are established in respect of the ICT security implications of personnel changes. Suitable measures are applied that provide for continuity of ICT security when staff vacate or occupy a post:
-a record that new staff have been issued with, have read the appropriate documentation relating to ICT security, and have signed the list of rules;
- a record that those rights have been amended or withdrawn due to a change to responsibilities or termination of employment.
• The school maintains the right to regularly monitor internet traffic, the school's network and user email. We are obliged to monitor to fulfill our responsibilities with regards to UK law.

2.1.2 Passwords
All users must log in to the school LAN and the internet using user name and password provided. These must be kept secure, and no-one should give their user details to another to use. Any limitations in log in should be notified to the network administrator immediately. Breach may mean access is denied.

• All users must observe password protocols for network and internet access.
• Users must not reveal their password to anyone, apart from authorised staff. Users who forget their password must request the system manager to issue a new password.
• A password must be changed if it is affected by a suspected or actual breach of security or if there is a possibility that such a breach could occur.
• Users should not share logins or passwords.

Visitors to the network will also be given a user name and password. These will be rescinded when the visitor leaves. Any files or documents will be kept for a short while, up to 3 months, and then deleted from the system.

All machines should be locked or logged out when unattended. Staff should also follow the policy of the school for security of the premises and equipment on it.

2.1.3 Private hardware and software
• Dangers can occur from the use of unlicensed software and software infected with a computer virus. It is therefore vital that any private software permitted to be used on the school's equipment is acquired from a responsible source and is used strictly in accordance with the terms of the licence. The use of all private hardware for school purposes is approved by the System Manager.
2.1.4 Equipment positioning

- Reasonable care is taken in the positioning of computer screens, keyboards, printers or other similar devices. Wherever possible, and depending upon the sensitivity of the data, users observe the following precautions:-
- Devices are positioned in such a way that information stored or being processed cannot be viewed by persons not authorised to know the information. Specific consideration should be given to the positioning of devices on which confidential or sensitive information is processed or retrieved.
- Equipment is positioned to avoid environmental damage from causes such as dust & heat.
- Users have been instructed to avoid leaving computers logged-on when unattended if unauthorised access to the data held can be gained. Clear written instructions to this effect should be given to users. Users should not allow other staff or children to access their account. Computers programmed to log out after a certain time period.
- Users have been instructed not to leave hard copies of sensitive data unattended on desks.

The same rules apply to school equipment in use at a user's home.

2.1.5 Virus Protection

- Biddick Hall Junior School uses appropriate Anti-virus software for all school ICT systems.
- Biddick Hall Junior School ensures that every ICT user is aware that any PC with a suspected or actual computer virus infection must be disconnected from the network and be reported immediately to the System Manager who must take appropriate action, including removing the source of infection.
- Any third-party laptops not normally connected to the school network must be checked by the System manager for virus's and anti-virus software before being allowed to connect to the network.

2.1.6 Disposal of equipment

- Disposal of waste ICT media such as print-outs, data CD's etc is made with due regard to sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it can be derived.
- Prior to the transfer or disposal of any ICT equipment the System Manager ensures that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply. Any ICT equipment must be disposed of in accordance with WEEE regulations.

2.1.7 Repair of equipment

- If a machine, or its permanent storage (usually a disk drive), is required to be repaired by a third party the significance of any data held must be considered. If data is particularly sensitive it must be removed from hard disks and stored on a portable drive for subsequent reinstallation, if possible. The school will ensure that third parties are currently registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

2.2 Communication Systems

2.2.1 Email Use

You must use the e-mail address issued by the school for employment purposes only.

You may not send e-mail to any user who does not wish to receive it. Users must refrain from sending further e-mail to a user after receiving a request to stop.

Chain letters, flood e-mails and mail bombs may not be propagated using the Service. You may not operate or assist in any way whatsoever any web site, email address, email service, ftp service or any other online service, which is advertised or promoted by means of Unsolicited Bulk Email

You may not use false e-mail headers or alter the headers of e-mail messages to conceal their e-mail address or to prevent Internet users from responding to messages. You may not use any email address that you are not authorised to use.

E-mail sent through the school service is deemed to be representing the school. As such any e-mail must not contain defamatory remarks, offensive language or other inappropriate material.

Attachments may only be opened if you are certain they do not contain any virus or other damaging content.

Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Any digital communication between staff and students / pupils or parents / carers (email, text, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking platforms must not be used for these communications.

Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Pupils at KS2 and above will be provided with individual school email addresses for educational use.

2.2.2. Managing approved Email Accounts

- All users who log on to the learning platform and school email system at home or at any other location, must only use these systems for educational use and are bound by the acceptable use guidelines.

- The school has the right to monitor e-mails and internet use.
- No users should ever use the school's communication systems to access or send inappropriate materials such as pornographic, racist or offensive material or to send or forward anonymous messages and chain letters.
- Users should not access public chat rooms and messaging systems (social networking sites)
- Users should not use the school's communication technologies for personal financial gain, gambling, political purposes or advertising.
- Users will be advised to never disclose personal details such as name, address, age or telephone number.
- Any inappropriate communications received must be reported to a member of staff immediately.

2.2.3 Accessing Internet Sites

All access to the Internet is filtered with an industry standard solution.

The school will monitor internet sites visited and may prohibit access to some sites deemed unacceptable or inappropriate.

All Internet usage on the network is monitored and logged and a log is kept of all sites visited. When specific circumstances of abuse warrant it, individual web sessions will be investigated and traced to the relevant site and user account. Such an investigation may result in action and possibly criminal investigation.

Copyrights and licensing conditions must be observed when downloading software and fixes from the web sites of authorised software suppliers. Such files must never be transmitted or redistributed to third parties without the express permission of the copyright owner.

The laws of all nation states, regulating such diverse subjects as intellectual property, fraud, defamation, pornography, insurance, banking, financial services and tax, apply equally to on-line activities.

Documents or material must not be published or accessed on the web which are defamatory or which may constitute intimidating, hostile or offensive material on the basis of sex, race, colour, religion, national origin, sexual orientation or disability under the sovereign law of the country in which the web server hosting the published material is sited.

- Users should not visit sites that contain illegal, obscene, hateful or other objectionable material.
- Users should use the school's internet for professional/educational purposes only and not for personal reasons within school time.
- At Key Stage 2, pupils should not be allowed to 'surf' the internet freely. They should be given specific sites to access or clearly defined and closely directed activities.

2.2.4 School Web Site

The following protocols will be observed:-

• Staff and pupil contact information will not generally be published. The contact information given, will be that of the school office.

• Pupils' names will not be used.

• The permission of parents will be sought, before photographs or work are published on the school website.

2.2.5 Managing videoconferencing & webcam use

The school takes part in communications with other schools via video conferencing or dedicated websites. This must only be done with teacher supervision. The school only uses secure access.

• Videoconferencing should use the educational broadband network to ensure quality of service and security.

• Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

• Videoconferencing and webcam use will be appropriately supervised for the pupils age.

• Webcams should be checked and monitored to ensure that misuse does not occur accidentally or otherwise.

2.2.6 Social networking, instant messaging and personal publishing

The term 'social networking' refers to online communities where typically text, photos, music, video are shared by users. Instant messaging refers to online chatting to others in 'real time'.

• The school will not allow adults and pupils access to social networking and instant messaging sites.

• Staff, pupils, parents and carers must not put photographs of other people from the school community on social networking sites without their permission.

• Newsgroups will be blocked unless a specific use is approved.

• The school does accept that there can be educational benefits (e.g. collaborative work nationally and internationally) and will therefore examine their use for teaching and learning as the need arises.

• The school will consider how to educate pupils in their safe use.

-Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

-Pupils will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

-Pupils will be advised to use nicknames and avatars when using social networking sites.

2.3 Protecting Personal Data

• Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and 2018, and in line with GDPR.

2.4 Copyright and Plagiarism

• The school will ensure that copyright and intellectual property right laws are not infringed.

• Pupils will be taught to reference all material used from the internet and other sources, as they develop their research skills.

3. Mobile Devices

3.1 Taking digital images using cameras and videos

It is recognised that the taking of digital images is an integral part of the teaching and learning experience, but there must be a clear educational reason for creating, storing, distributing and/or manipulating images of members of the school community.

- Staff and pupils may take digital photographs or videos using school equipment, on school visits).
- All images of children stored on the school network or on staff laptops should be placed in a common folder with a clear explanation of the intended use of the images, not in the
- Pupils' names should not be used when saving images.
- Pupils will be taught how images can be misused, through their e-Safety learning.

3.2 Mobile phones

- Pupils should not bring mobile phones into school. In exceptional circumstances the phone will be stored in a central place until home time.
- Pupils will be advised that the sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

3.3 Ipads/portable devices

- If school Ipads/portable devices are taken home, staff are responsible for their security.
- School ipads are for sole use of the staff member to which they are loaned.
- The school IT technician is responsible for maintenance of school Ipads/portable devices and no other person should tamper with them.

3.4 Portable Storage Devices

- All staff are provided with encrypted portable hard drives.
- All users are responsible for the security of mobile storage devices.
- Pupils are not allowed to use their own devices.

3.5 Data

- We use google drive, the network or an encrypted portable hard drive to store sensitive data (assessment and Sen).
- We use an encrypted email system (egress) to send and retrieve sensitive data.
- An encrypted hard drive is used to transport data from home to school.

3.6 Games Machines

- Staff should check that gaming software is age appropriate if machines are allowed (e.g. fun/toy days), as outlined by PEGI ratings.

3.7 DVD

- These should be age appropriate, as outlined by the film classification authority**.**

4. Assessing Risks and Handling e-Safety Issues

4.1 Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material.

However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.2 Reporting Procedures

4.2.1 Reporting Accidental Access to Inappropriate Material

Any user of the school and/or Durham County Council network who accidentally comes across inappropriate or offensive material should do the following:

1. Inform the e-Safety coordinator of the incident and give the website address.
2. Log the web address, time and username in the e-safety incident log.
3. The school should block the website via its own filtering solution.
4. The e-Safety co-ordinator should contact the LA e-Safety contact for schools.

4.2.2 Reporting Accidental Access to Illegal Material

Any User of the Durham County Council Network who accidentally comes across illegal material should do the following:-

1. Report the incident to the e-Safety coordinator.
2. Do not show anyone the content or make public the URL.
3. Make sure a reference is made of the incident in the e-Safety incident log.
4. Go to the IWF website at www.iwf.gov.uk and click the report button.
5. If reporting a URL do not use copy and paste, type the URL.

4.2.3 Reporting Suspected Deliberate Abuse or Misuse

Any person suspecting another of deliberate misuse or abuse of the regional broadband network should take the following action:

1. Report in confidence to the Head teacher.
2. The Head teacher should inform the Local Authority.
3. The Local Authority should complete an internal RIPA form, requiring Durham County Council to complete an internal investigation.
4. If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Durham County Council will inform the relevant police authority who will complete their own investigations.
5. If the investigation confirms that inappropriate behaviour has occurred, Durham County Council will inform the relevant authority. This may be the Local Authority or the School's Board of Governors.
6. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Examples of Inappropriate Use:

- Visiting pornographic sites (adult top shelf materials)
- Causing offence to religious groups
- Inappropriate use of email
- Deliberate sabotage of the network; i.e. hacking, mail bombing etc.

4.2.4 Access to Illegal Material

If this investigation results in confirmation of access to illegal materials or the committing of illegal acts, Durham County Council will inform the relevant police authority that will complete their own investigations and a criminal investigation may follow.

Examples of Illegal Acts:

- Accessing any child abuse images.
- Incitement to racial hatred
- Incitement to violence
- Software media counterfeiting or illegitimate distribution of copied software.

4.3 Sanctions

- Sanctions for the abuse or misuse of school ICT systems will be determined by the senior management team or the e-safety Co-ordinator and governors of the school, as deemed appropriate.

4.4 Key contacts:

Mike Hamilton (LA e-Safety Contact for Schools)
Tel: 0191 4246336 email: mike.hamilton@ictinschools.org

5. Authorising Access

5.1 Authorising access to the Internet and other ICT resources.

- All staff and pupils must read and sign an Acceptable Use Policy before using any school ICT resource.
- Parents will be asked to sign and return a consent form relating internet access and the taking of digital images.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will be asked to sign an acceptable use of school ICT resources before being allowed to access the internet from the school site.

5.2 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

6. Communicating this Policy

6.1 Introducing the e-safety policy to pupils

- A programme of training in e-Safety (in its broader sense) will be developed and embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.
- E-safety rules for school systems and equipment will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

6.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT will work with management and the LEA to establish clear procedures for reporting issues.

6.3 Enlisting parents' and carers' support

- Parents and carers will be referred to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents and carers will be offered advice on e-Safety on an individual or group basis.

7. E Safety Education

7.1 Students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in e-safety is therefore an essential part of the school's e-Safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.
E-Safety education will be provided in the following ways:

- A planned e-Safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school
- Key e-Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- 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 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- 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.

7.2 Parents/Carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. “There is a generational digital divide”. (Byron Report).
The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings

7.3 Staff

It is essential that all staff receive e-Safety training and understand their responsibilities. Training will be offered as follows:

- A planned programme of formal e-Safety training will be made available to staff. An audit of the e-Safety training needs of all staff will be carried out regularly.
- All new staff should receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The e-Safety Coordinator (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by LA and others.
- This e-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The e-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

CHILDREN, ICT AND E-SAFETY
Information for Parents and Carers

E-SAFETY IN SCHOOL

As part of our safeguarding procedures in school our school network is protected by the E-Safe Monitoring System. This software scans the school network detecting any inappropriate use, identifying any text or images that are unsuitable for children. This includes any text typed by the children. The school receives reports of any inappropriate use.

Simple rules for keeping your child safe at home
They should

- Ask permission before using the internet
- Only use websites chosen together or use a child friendly search engine
- Only e-mail people they know
- Ask permission before opening an e-mail sent by someone they don't know
- Not use internet chat rooms or chat functions on game consoles
- Not to use their real names when using games on the internet and online games such as X-Box Live
- Never give out a home address, phone number or mobile number
- Never tell someone they don't know where they go to school
- Never arrange to meet someone they have "met" on the internet

Useful Websites

When searching the internet we recommend you use one of the child friendly engines

1. Ask Jeeves for Kids http://www.searchbox.co.uk/kids.htm
2. www.swiggle.org.uk
3. https://www.kiddle.co/

Useful Tips

- Regularly check the websites your child is using
- Discuss these rules with your child

For further information go to

- CEOP: www.ceop.gov.uk
- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet-int.org
- UKSIC https://www.saferinternet.org.uk/
- Internet Matters https://www.internetmatters.org/

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

=

Biddick Hall Junior School

Acceptable Use Agreement for staff

- I have read a copy of the school’s e-safety/acceptable use policy.
- I will only use the school’s email / internet / intranet for professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will only use the approved, secure email system(s) for any school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to the e-Safety Coordinator.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school’s network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / internet that does not have up-to-date version of anti-virus software.
- I will not use personal digital cameras or camera phones for transferring images of pupils or colleagues without permission.
- I will ensure I am aware of digital safe-guarding issues so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access email / internet / intranet.
- I understand that all internet usage will be logged and this information could be made available to my manager on request.
- I agree and accept that any computer or device loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

Staff to sign sheet to clarify they have read and understood situated in STAFF ROOM.

Biddick Hall Junior

e-safety/AUP Policy

JANUARY 2018

Please sign once you have read this policy

M.Collinson

NAME	**POSITION**	**SIGNATURE**
MICHELLE COLLINSON	HEAD	
JENNY O'NEILL	DEPUTY	
CLARE LYNN	CLASS TEACHER	
FAYE DAVIES	CLASS TEACHER	
LINDSAY RENNIE	CLASS TEACHER	
GILL DRAKE	CLASS TEACHER	
KATH JONES	CLASS TEACHER	
BEVERLEY ARCHER	CLASS TEACHER	
DAN TROTTER	CLASS TEACHER	
ANDREW EDDON	CLASS TEACHER	
NICOLA WALLS	CLASS TEACHER	
NICOLA GIVENS	CLASS TEACHER	
SHELLY DENTON	CLASSROOM ASSISTANT	
PAULA YORSTON	CLASSROOM ASSISTANT	
KATHERINE ROCHFORD	CLASSROOM ASSISTANT	
ANGIE FINN	CLASSROOM ASSISTANT	
LILLIAN LAWS	CLASSROOM ASSISTANT	
DEBORAH STONEHOUSE	CLASSROOM ASSISTANT	
CAROL HENTON	CLASSROOM ASSISTANT	
MICHELLE TENNYSON	CLASSROOM ASSISTANT	
CHRISTINE DIXON	CLASSROOM ASSISTANT/ MIDDAY SUPERVISORY ASSISTANT	
CLAIRE HARTLEY	MIDDAY SUPERVISORY ASSISTANT	
SARA BLAKEY	CLASSROOM ASSISTANT/MIDDAY SUPERVISORY ASSISTANT	
GERALDINE HALL	MIDDAY SUPERVISORY ASSISTANT	
ANN ROBINSON	SECRETARY	
PAULA REED	CARETAKER	