Brackenwood Infant School

E – Safety Policy

		Name	Signature	Name	Signature
Date Adopted					
Review Date					

Contents

Communicating our E-Safety Policy

Appendices

Our E-Safety Policy

The E-Safety policy at Brackenwood Infant School relates to other policies for computing, bullying and for child protection.

Brackenwood Infant School's E-safety Co-ordinator is Mr Alex Smith (Computing Lead) and Mr Christopher Mervyn (Headteacher) is the Child Protection co-ordinator.

Introduction to E-Safety

1.1 E-Safety in a Changing World

The term E-Safety covers the issues relating to young people and staff and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

E-Safety should be applied to protect children, staff and all members of our school community. Our School's E-Safety Policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

At Brackenwood Infant School, we celebrate the value and importance of technology in our children's learning. In our school; personal computers, wireless laptops and iPads are all part of the children's every day learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies and the Internet on a daily basis and experience a wide range of opportunities and situations.

Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use.

Recently we have:

 Updated our wireless technology throughout the whole school.

 Purchased 30 iPads and leased another 30.

 Launched our new school website.

This year we have aspirations to:

 Continue to update our school website as a learning tool for use in school and at home.

 Increase pupil competency, awareness and knowledge of E-Safety in school.

Throughout our pupil's time at Brackenwood Infants we aim to:

 Use technology even more to enhance learning experiences,

 Use Computing technology to bring the outside World into the classroom.

 Ensure that all pupils are equipped with the knowledge and skills to be successful when using information communication technology and keep themselves safe.

Effective Practice in E-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented E-Safety Policy;

- A well thought out approach regarding how to develop E-Safety guidance within the school's curriculum.
- Identified opportunities to ensure that we support families with the challenges relating to E- Safety in the digital age (family workshops, web-links etc).
- Secure, filtered broadband from Wirral Council's Network;
- A school network that complies with the National Education Network standards and specifications, which are designed to protect our children online.

1.2 E-Safety and the Legal Issues

The renewal and updating of the E-Safety policy falls in line with the school's policy renewal cycle.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism, access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example, it is a criminal offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children. In addition, there are many grey areas for schools to consider regarding communication of social network sites, storage of data etc.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school, in consultation with Hi – Impact technicians, ensures that;

It has effective firewalls and filters on our school network.

- Ensures that e-safety responsibilities are clearly communicated to all members of our school community.
- That our Acceptable Use Policies are fully enforced for children, staff and visitors.
- Ensures that our procedures are consistent with the UK General Data Protection Regulation Act and the Data Protection ACT (2018).

- That school has up to date GDPR (UK) policies and that these are understood and followed by all members of staff and children.

Learning and Teaching in the Digital Age

The school uses wireless laptops and iPads and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology and safely

2.1 Why the Internet and digital communications are important

Mobile Communication equipment and the Internet are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication from an early age. It is part of their lifelong learning experiences and habits. We have to embrace that opportunity. However, we also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

In addition, the use of the Internet is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2 Encouraging responsible use of the Internet and digital communication.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.

- Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication.
- Pupils will be taught what Internet use is acceptable and what is not. They will be given clear objectives for Internet use.
- Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy and authenticity.
- Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites, we must also ensure that our children know how to manage the risks and dangers associated with these activities.

Managing Digital Access, Communication and Content

All Internet accessed is managed by the school. The school recognises that password protection is a vital element of promoting e-safety.

The school will ensure that permission for access and use of any content including photographs and video is fully explained and sought on admission to the school.

3.1 Information system security

- School computing systems security will be reviewed regularly. This will be part of the liaison between the Computing Lead and Hi Impact Education Consultants.
- Virus protection will be updated regularly as part of the school's Service Level Agreement with Hi Impact.
- Security strategies will be discussed with the Local Authority.

3.2 Managing filtering

- The school will work with Hi-Impact to ensure systems to protect pupils are reviewed and Improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-Safety Coordinator Mr. Smith.
- Hi-Impact technicians will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.3 E-mail

- Staff should only use school approved e-mail accounts at work. Clear guidance for what constitutes professional use of e-mail is included in the Acceptable Use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

3.4 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a senior member of staff.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.5 Publishing pupil's images

- Photographs that include pupils will be selected carefully. The school will always risk assess/review photographs for possible abuse.
- Full names of pupils or any other personal details will never be published alongside photographs.
- Pupils' full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing. **(Appendix 7)**

3.6 Social networking and personal publishing

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. The school will use age appropriate resources to teach children about social interaction and communication on the Internet. This should be carefully managed. All staff will seek the approval of the head teacher before using any sites with children.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for Key Stage 1 aged pupils.
- Staff are fully informed of their responsibilities regarding the use of social networking sites such as Facebook. At Brackenwood Infant School, we have agreed that it is good practice to separate professional and personal commitments and comments. Therefore, the following groups should not be allowed as contacts and friends on social networking sites;
    - **Ex pupils or current pupils** - the context of teacher to pupil relationship is not suitable for social networking.
    - **Parents** - We believe that it is unfair on parents and staff to complicate the professional relationship that exists within school through the use of social networking sites. It is both inappropriate and open to abuse.
- All staff are also aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.
- Staff are also aware that they are responsible for the security protocols regarding any social networking accounts. This is a professional responsibility. **(Appendix 5)**

3.7 Managing videoconferencing & webcam use

- At Brackenwood Infants we will only use webcams for specific projects and full consent will be sought before children participate in these.
- Video conferencing should use the educational broadband network to ensure quality of service and security. Video conferencing for pupils can only take place under the direct supervision of a member of staff.
- All software for webcam use will be password protected.
- At Brackenwood Infant School, we will always seek consent from parents for any video conferencing events our children are involved in. **(Appendix 3).**

NEU Cyber-Safe guidance states all staff should;

- Not post information and photos about themselves, or school-related matters, publicly that they wouldn't want employers, colleagues, pupils or parents to see.
- Keep passwords secret and protect access to accounts.
- Not befriend pupils or other members of the school community on social networking sites. (Staff should consider carefully the implications of befriending parents or ex-pupils and let school management know if they decide to do this.)

National Association of Schoolmasters Union of Women Teachers (NASUWT) guidance states:

Most social networking sites allow users to apply privacy settings to control how public or private the information that they post online will be. Before posting information or images on social networking sites:

- check the privacy settings and adjust them to ensure you do not risk sharing information about yourself or others (e.g. your family or colleagues) with people you do not want to;
- review your privacy settings regularly;
- bear in mind that on some social networking sites, people that are not your approved 'friends' will still be able to see some of the information you post online;
- use strong passwords and logins to prevent unauthorised access to your social networking account and privacy settings;
- choose a user name that does not include any personal information;
- avoid posting personal information about yourself – either in your profile or in your posts (e.g. telephone numbers, pictures of your home, workplace or school, home address, birthday, holiday plans) – that could make you vulnerable to identity fraud, theft or harm;
- think carefully before posting information which other people might be able to access and use against you – for example, your employer or a potential employer, or a colleague, parent or pupil;
- obtain consent from other people (especially colleagues, parents and pupils) before uploading their pictures or personal information;
- have separate social networking accounts for your work and personal activity online;
- beware of 'phishing' scams, including fake 'friend' requests and posts from individuals or organisations inviting you to visit other pages or sites;
- ensure you have effective and updated antivirus/antispyware software and a firewall running before you go online.

Ensuring privacy online

- Ensure you always have effective and updated antivirus/antispyware software running on your computer.
- Only use secure wi-fi networks and ensure your home network is also secured.

- Do not leave your computer, smartphone or tablet unattended in public places. If you are using your computer, smartphone or tablet in a public place, be aware that there will be other people around you who may be watching what you are doing online.
- Unless you are using a secure web page, do not send or receive private information when using public wi-fi.
- Only use secure websites when making transactions online, including when banking online, checking personal information records, or when reviewing any private, sensitive or confidential information online.
- Always log out of secure websites as soon as you have completed a transaction and before you log out or turn off your computer/device. Closing the window or shutting down your computer may not automatically log you out of the website you have visited and may make your information accessible to someone else who might be using the same computer/device.
- Always use strong passwords (a mixture of lower and upper case letters and numbers) and change your passwords regularly. You should never reveal your password to anyone else.
- Keep passwords and wi-fi codes safe so that others cannot access or use them. Check what data is stored about you, including data about you using cloud storage. Find out about what controls are in place to ensure the security and integrity of data about you.
- Check whether information held about you might be used for direct marketing purposes. If you have any concerns, you have the right to stop your information being harvested or passed to other organisations for the purpose of direct marketing.
- Use search engines (e.g. Google, Bing) to check for any information that may have been posted online about you. Contact the author, website administrator or search engine provider to have any inaccurate or malicious information removed.
- Do not use a work e-mail address for personal use. It is far better to have a separate, private e-mail address for private use. Where personal information is transmitted using a work e-mail address or using a computer/device or network provided by your employer, it may be accessed by your employer at any time.
- Use any computers/devices provided to you by your employer solely in accordance with the provisions of the employer's Acceptable Use Policy, and not for your own personal purposes.
- Keep work-related devices and systems separate from devices used for personal/private purposes at all times.
- Avoid swapping data storage peripherals between work and personal computers/devices, especially without undertaking appropriate antivirus checking.
- Do not access links to unknown or bogus websites or open e-mails from unknown or suspicious sources.
- Do not provide personal or private information in response to unsolicited telephone calls.
- Check privacy settings and adjust them to ensure you do not risk sharing information about yourself or others (e.g. your family or colleagues) with people you do not want to.
- Do not use unsecured wi-fi networks whether in your home, office or when out and about.
- Ensure your wireless hub/router is secured so that other people cannot easily gain access to sensitive information that you may be sending or receiving online. This is an important precaution when you are working and using your own equipment to communicate online. Simply search for available wireless networks, and those that are secured will be indicated with a padlock symbol.

- Check that your device does not auto-connect to wi-fi signals. If your device is set to automatically connect to available open wi-fi networks, then you run the risk of automatically connecting to unknown and potentially dangerous networks. You should switch off auto-connect via the device settings.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Staff are allowed to have mobile devices in school but these must not be used during working hours except for school or emergency based communication in office areas or the staffroom and PPA room **(Appendix 6)**
- The senior leadership team should note that technologies such as mobile devices with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Personal mobile devices will not be used during lessons or formal school time.
- The use by pupils of cameras in mobile devices is not allowed. **See mobile phone policy in appendix 6 for further details.**
- Staff will be issued with a school phone where contact with pupils is required or school camera to capture photographs of pupils. Staff must not take photographs on their personal phones.
- The appropriate use of Learning Platforms will be discussed with Hi-Impact Education consultants termly

3.9 Protecting and storing sensitive data including images

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
- Photographs should only be accessed in school and should be moved into the school media storage folder and deleted from the device also.
- All data and images of children must be stored in the staff shared area on the curriculum network or the school's secure administration network.
- Photographs cannot be stored on personal laptops.
- No data or images can be transported out of the school without the device being approved or password protected.

3.10 Use of Photographs

The Data Protection Act (2018) affects our use of photography. This is because an image of a child is personal data for the purpose of the Act and it is a requirement that consent is obtained from the parent of a child or young person under the age of 18 years for any photographs or video recordings for

purposes beyond the school's core educational function. (E.g. school web sites, school productions). At Brackenwood Infant School we seek permission for all photography and video use.

There will also be times where the school will be carrying out off-site activities e.g. educational visits. Our guidelines are created to make sure that all images are taken appropriately by both adults in the school and children taking part in visits.

For both school / setting and other events which are photographed for publicity purposes additional consent should be sought from the child's parent/guardian or the child and kept on file covering all cases where images of children are to be published beyond the parameters of school use.

Where children are 'Looked After' schools must check consent on the corporate parent's behalf with the social worker and there may be other situations, (in adoption placements or following a resettlement from domestic violence for example), where a child's security is known by the class teacher to be at stake, indicating the need for extra care.

Consent is sought for the whole time that children are at Brackenwood Infant School. Parents retain the right to withdraw consent at any stage, but they need to do so in writing. **(Appendix 7)**

3.10a Planning photographs of children

Images and details of pupils published together allow for the remote possibility that people outside the school could identify and then attempt to contact pupils directly. The measures described below should help to minimise the risk of such unsolicited attention.

- Use images of children in suitable dress, and take care photographing PE events to maintain modesty, using team tracksuits if appropriate for example, photographs should not be taken of swimming pool based events.
- Remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your school as an inclusive community, and to comply with the Disability Discrimination Act.
- Decide whether parents and visitors will be permitted to take photographs of the event. This must be authorised.
- On school trips, parents may take photos of children but only with school iPads and under guidance from staff.

3.10b Identifying children

If the pupil is named, avoid using their photograph. If the photograph is used, avoid naming the pupil.

It is our policy that:

- You use the minimum information. Ask yourself whether it is really necessary to accompany a picture with the pupils' names, the year group, or the school.
- When fully naming pupils in any published text, whether in the school's brochure, website, or in the local press, avoid using their photograph, unless you have parental consent to do so.

3.10c Using photographs of children supplied by a third party

When using third parties, it is our school's responsibility to check that the adults are aware of the school protocols. In addition we would expect that the adult taking the images has a full DBS or is supervised when taking images by a member of the school's staff.

Children should never be left alone with a photographer.

Copyright does not apply to images for private family use. However, copyright does exist in commercial photographs and it rests with the photographer. Copyright is a right that the photographer automatically enjoys as the creator of the work to prevent other people exploiting their work and to control how other people use it. If you commission photographs for use at a school/setting or work include in your contract that the school will own the copyright for items taken on your behalf.

3.10d Use of Images of children by the Press

(Please refer to the recommendations in section 3.10b above; 'Identifying Pupils')

There may be occasions where the press take photographs at school of pupils. If this occurs, we will ensure that specific permission is sought from the parent about whether to agree to their children being featured in the press and whether their full name should accompany the photograph.

3.10e Videos

School will ensure that parental consent is in place before any child can appear in a video, Parents can make video recordings of nativity plays and other such events for their own personal and family use, as the Data Protection Act does not cover them. (Please refer to section 3.10h).

3.10f Websites

Website use can be of particular concern to parents and staff because of the potential misuse of images by paedophiles. With digital photography, there is the remote possibility that images of children could be produced, manipulated and circulated without the parents or children's knowledge. The dual concern which follows such a risk is that children might be exploited and a school or setting might be criticised or face legal action. Images on a website can be made more difficult to copy by several measures - copy-protection, overlaying with a watermark, or published in low definition.

It is important to take care with identification and to respect parental views on the use of any photography of children on a website.

Increasingly adults and children are generating content for websites e.g. children and adults placing pictures on **Twitter and Facebook** web sites. It is therefore important that schools/organisations ensure that children, staff and parents understand the risks involved and are encouraged to adopt safe practice when generating content for school related websites.

This is included on our permission forms. Parents and staff are not allowed to share school images on any Internet sites.

3.10g Webcams

The regulations for using webcams are similar to those for CCTV (closed-circuit television). This means that the area in which you are using the webcam must be well signposted and people must know that the webcam is there before they enter the area, in order to consent to being viewed in this way. Children should be consulted and adults would need to consent as well as the parents of all the affected children.

In gaining consent, the school must tell the person why the webcam is there, what you will use the images for, who might want to look at the pictures and what security measures are in place to protect access.

3.10h Parental right to take photographs and videos

We want parents to have the opportunity to record school events safely and responsibly.

We will allow recording, unless we feel that the images created may be inappropriate. We also have to ensure that consent is gained for all children taking part.

Parents are not covered by the Data Protection Act 2018 if they are taking photographs or making a video recording for **their own private use**. The Act does not, therefore, stop parents from taking photographs or making video recordings at school events, such as nativity plays or other such performances.

Parents are not permitted, however, to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of a school event). Recording and/or photographing other than for private use would require the consent of the other parents whose children may be captured on film. Without this consent the Data Protection Act 2018 would be breached. **The consent form attached reminds parents of this fact**.

3.10i Images taken by young people

Children do have permission to take photographs on school trips using assigned iPads but only when monitored. We will ensure that children understand that photographs must be responsible and not taken in private places.

3.10j Use of Mobile Phones

Children are not allowed to use mobile phones in school.

Staff are not allowed to video or take photographs of children using mobile phones as the data is not easily transferrable and may breach our obligations under the Data Protection Act.

Visitors are also informed of this as part of our safeguarding statement. Parents can use them for recording only based on the guidelines above**. (Appendix 6)**

4.1 Authorising Internet access

- All staff must read and sign the 'Agreed Staff Code of Conduct to promote E-safety and Responsible Use**' (Appendix 1)** before using any school computing resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- All Parents/Carers will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign an 'Acceptable use of school computing resources**' (Appendix 4)** before being allowed to access the internet from the school site. This includes governors, visitors, student teachers etc.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material and will consult Hi –Impact in order to assess any potential risks. 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. Neither the school nor LA can accept liability for any material accessed, or any consequences of Internet access.

- The school audits computing use to establish if the e-safety policy is adequate and up to date. Mr Smith (Computing lead) will ensure that the implementation of the E-Safety policy is appropriate and effective.

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a safeguarding nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints policy)
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police to establish procedures for handling potentially illegal issues.

4.4 Community use of the network and Internet

- Through extended schools use and partnership with other organisations there will be wider community use of the school's network. The school will liaise with local organisations to establish a common approach to e-safety.

Communicating the E-Safety Policy

5.1 Introducing the e-safety policy to pupils

- Cyber bullying and E-Safety rules will be posted in all classrooms and read to pupils when covering E-Safety during Computing lessons **(Appendix 2).**
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- E-Safety training will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.

5.2 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 Computing use will be supervised by senior management and work to clear procedures for reporting issues.

5.3 Enlisting parents' and carers' support

- Parents and carers attention will be drawn 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. Parents and carers will be sent parental guidance for how to encourage E-Safety at home as well as in school.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

This policy will be reviewed annually or in line with legislation changes.

Appendix 1:

Agreed Staff Code of Conduct to promote E-Safety and Responsible Use

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. Brackenwood Infant School expects that all activity should be related to a professional use.

I appreciate that ICT includes a wide range of systems, including mobile phones, smart devices and/or tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school. I also understand my responsibilities regarding the use of photographs and videos and how to store these.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely and is used in line with GDPR (UK) law, whether in school, taken off the school premises or accessed remotely. I understand that images of children from school cannot be stored on laptops.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the E-Safety Coordinator, the Designated Safeguarding Lead or Headteacher.

I will ensure that electronic communications with pupils and parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I fully understand my professional responsibilities, if I chose to use Social Networking Sites.

I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for Computing.

Signed:_____ Date: _____

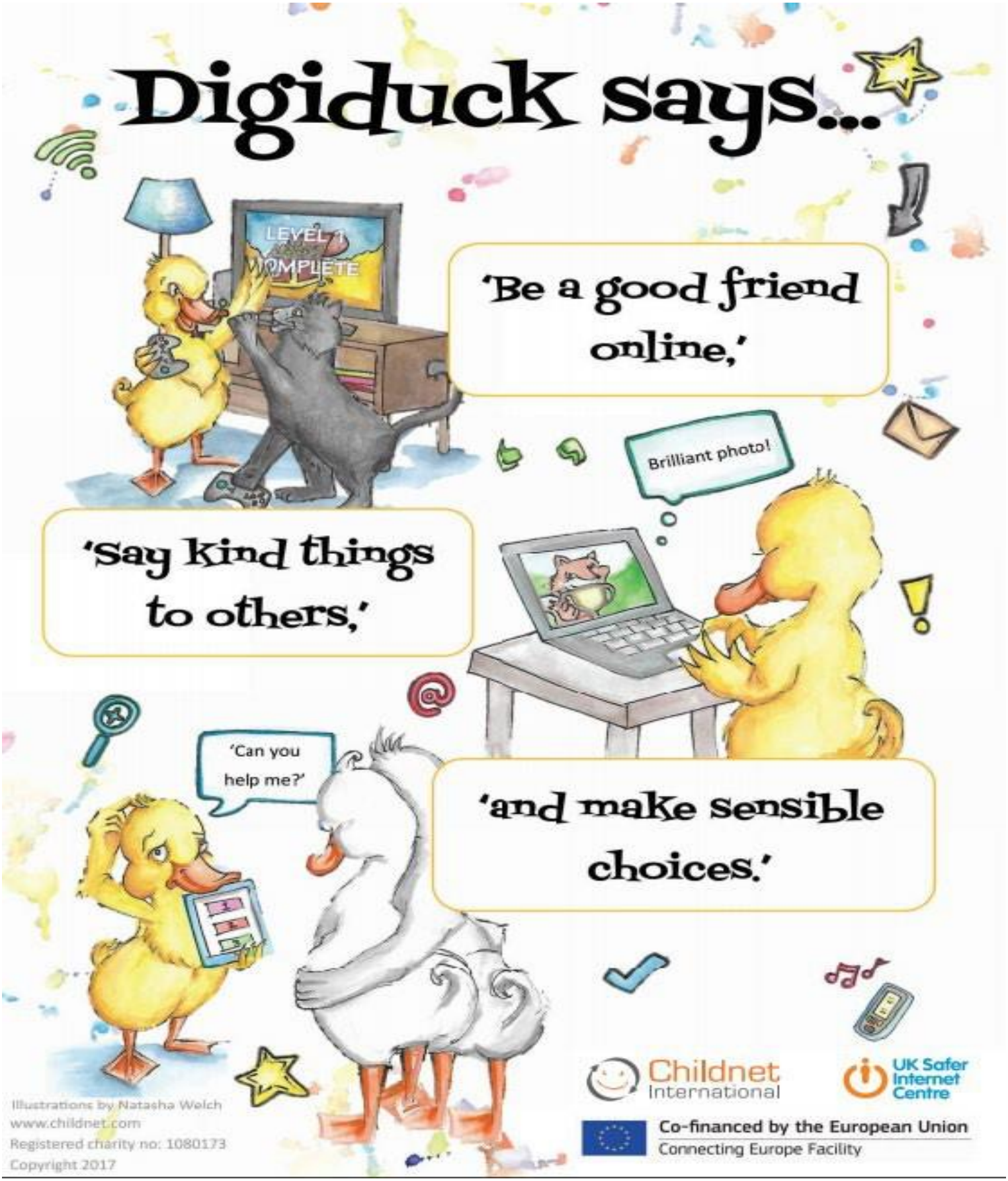
Appendix 2 – **Key Stage 1 Internet Safety Rules**

Think Then Click!

These rules help us to stay safe on the Internet

	We only use the internet when an adult is with us.	
	We can only tap on the icons or links when we know what they do.	
	We can search the Internet with an adult.	
	We always ask if we get lost on the Internet.	
	We can send and open emails together.	
	We can write polite and friendly emails to people that we know.	

Appendix 2 –F2 Cyber bullying rules



Appendix 3 – E –Safety Rules consent form

Brackenwood Infant School

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/ carers are asked to sign to show that the e-Safety Rules have been understood and agreed and that permission is given for children to have their own individual log on accounts for school approved on-line learning platforms, for example, IXL and Bug Club.

Our E-safety policy is available from the school office and is published on the school's website.

Signed:	**Date:**

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

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.

Signed:	**Date:**

Class Webinars

I give permission for my child to be photographed or recorded as part of school and to be involved in classroom webinars

Signed:	**Date:**

I request permission to take photographs and video recordings of my child at authorised school events (performances, sports day etc) and confirm these are for my personal use only and will not be shared on any internet or social media sites

Signed:	**Date:**

Please print name: _____

Childs Name: _____

Please complete, sign and return to the School Office

Appendix 4: Visitors code of conduct for ICT

All adults have to be responsible when using information systems. As visitors to schools, adults have to be aware that their activities must be related to education or their role within the school (PTA administration, family learning etc). Any abuse of this privilege could result in access being removed. In cases where the school feels that either their pupils or staff have been placed at risk, this could lead to the incident being reported to the police.

All visitors should consult the school's E-Safety policy for further information and clarification. This is available through the school office or the school's website.

It is forbidden to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional and educational use. It is not appropriate to use social networking sites in school.

I appreciate that ICT includes a wide range of systems, including mobile phones, smart devices and/or tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.

I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that no files are removed from the school's network without the express permission of a senior member of the school's staff.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the Headteacher.

I will ensure that all e-mail communication is appropriate.

I will not access any inappropriate websites including social networking sites.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Visitor's Code of Conduct for ICT.

Signed:_____ Date: _____

Appendix 5 - POLICY ON THE USE OF SOCIAL NETWORKING WEBSITES

The purpose of the policy is to provide clarity to all school staff on the use of any social networking website, e.g. Facebook, Twitter, Bebo and its implications in relation to future employment status i.e. disciplinary action and potential dismissal. The policy relates to any young person under 19 years of age, any 'looked after child' under the age of 21 years of age, and any young person with special educational needs under the age of 24 years of age.

Any member of staff can have an account on a social networking web site. However, it is the responsibility of the individual to ensure that anything placed on the social networking site is appropriate and meets the standards expected of professional teachers and school support staff.

NB *School employees who have their own social networking site may have contact with relatives or family friends. However all the requirements below would still apply to the use of Social Networking Websites.*

All school staff **must:**

- Demonstrate honesty and integrity, and uphold public trust and confidence in respect of anything placed on social networking web sites.
- Ensure that any content shared on any social networking web site, at any time, would be deemed as appropriate, i.e. staff are personally responsible for ensuring that any privacy settings meet this requirement.
- Ensure appropriate language is used, at all times, for any comments placed on social networking sites.
- Ensure that any comments and/or images, at any time, could not be deemed as defamatory or in breach of any relevant legislation.

All school staff **must not:**

- Have contact with current/ex pupils, or other children or young people where there is a relationship developed as part of their 'professional' role, e.g. music tutor, on any social networking website.
- Use social networking sites as a forum to make derogatory comments which could bring the school into disrepute, including making comments about pupils, parents, other staff members, the senior leadership team, governors, local authority or the wider community.

Any breaches of this policy could result in disciplinary action and may result in your dismissal. I understand and agree to adhere to the Policy on the Use of Social Networking Websites.

Signed:	Date:

This document has been developed and consulted on with Wirral Professional Teachers' Associations and Trade Unions

Appendix 6

Use of Mobile Phones Policy

As part of our safeguarding commitments and E-Safety policies the school has adopted the following policy regarding the use of mobile phones at Brackenwood Infant School.

The strategies outlined in this policy are designed to ensure that the following does not occur; Use of mobile phones to take unauthorised photographs, videos or sound recordings of children. Mobile phones being used during working hours by staff.

Mobile phones being used by visitors in areas of learning.

Children and Mobile Phones

- Children are not allowed to have and therefore use mobile phones in school

Staff and Mobile Phones

- Staff are not allowed to use mobile phones during working hours. They must be turned off if you are on the school premises.
- Staff can use mobile phones for contacting the school office on work related calls. School may provide a work based mobile phone. These should be not be used in close proximity of children.
- We advise staff to call parents on the school phones or school mobile phones when possible.
- On residential trips, staff can use mobile phones outside direct hours of supervision, as long as it does not compromise the safety of the children.
- Mobile phones can be used during lunch hours, during breaks or outside working hours. These should not be used in the vicinity of children. We suggest that you use mobile phones in unoccupied classrooms, office areas, staff room or intervention rooms.
- Personal mobile phones cannot be used to take photographs, videos or recordings in school. This includes school trips and residential activities.
- Educational partners will be informed of these policies and asked to follow these guidelines.
- Staff are not allowed to give parents their personal mobile phone numbers. All communication with parents should be through the school e-mail system, professional meetings or using the school phone system.

These guidelines apply to all students and staff on trainee placements. Parents and Other Visitors using Mobile Phones

- Parents and other visitors are not allowed to use their mobile phones in school.
- If parents do need to make a call or send a message, they will be asked to step outside the school premises to make the call.
- Parents and visitors will be allowed to take photographs and videos on their phones at **authorised events** as long as they have completed the appropriate permission form.

We ask parents and visitors to not take any offence if a member of staff requests them to stop using their mobile phone.

Name:_____ **Signature:**_____

Brackenwood Infant School

Pulford Road, Bebington, Wirral, Merseyside, CH63 2HN
Email: schooloffice@brackenwood-infant.wirral.sch.uk
Tel: 0151 608 9117
Headteacher: Mr C. Mervyn

Appendix 7

I agree to consent to images of my child being used on the school's: -	**Agree**	**Disagree**
Website		
Twitter Feed		
Newsletters		
School prospectuses, flyers, leaflets and brochures		
Other promotional material (such as banners, signs and displays)		
Reporting events in newspapers and other media including		
Use by external companies (such as sports clubs)		
In and around the school building		
To photographs being taken of my child (individual and group photos) by the school photographer. The group photos will be made available for other parents to purchase.		

I consent to my child's images being used by the school in the media formats as set out above

Name of child : ……

Signature of parent / carer : ……

Date : ……