Humshaugh C. E. First School
e-Safety Policy

Authors: Jude Long and Revd. Steve Wilkinson

Policy Updated: January 2018

The Headteacher Jude Long is responsible for e-Safety in the school.
The Governor responsible for e-Safety is Revd. Steve Wilkinson

Policy approved by Head Teacher on: 19.1.17

Policy approved by Governing Body on: 20.1.17

The date for the next policy review is January 2019

Table of Contents

Background Information....3
End to End eSafety....3
Use of the CFE Core e-Safety Policy....3
Monitoring....3
Further Information....3
eSafety Audit....4
1 Writing and Reviewing....5
2 Teaching and Learning....5
2.2 How does Internet use benefit education?....5
2.3 How can Internet use enhance learning?....6
2.4 How will pupils learn how to evaluate Internet content?....6
2.5 Using the Internet....6
3 Managing Internet Access....7
3.1 Information system security....7
3.2 E-mail....7
3.3 The School Website....7
3.3.1 Publishing contact details....7
3.3.2 Publishing pupil's images and work....7
3.4 Social networking and personal publishing....8
3.5 Protecting personal data....8
3.6 How will filtering be managed?....8
3.7 How will video conferencing be managed?....8
3.8 How are emerging technologies managed?....8
4 Policy Decision....9
4.1 Authorising Internet access....9
4.2 Assessing risks....9
4.3 How will the school respond to any incidents of concern?....9
4.4 Handling e-Safety complaints....10
4.5 Community use of the Internet....10
4.6 How will Cyberbullying be managed?....10
4.7 How will Learning Platforms be managed?....11
4.8 How will mobile phones and personal devices be managed?....11
4.9 Pupils Use of Personal Devices....11
4.10 Staff Use of Personal Devices....12
5 Communications Policy....12
5.1 Introducing the e-Safety policy to pupils....12
5.2 Staff and the e-Safety policy....12
5.3 Enlisting parents' support....12

Background Information

e-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their on-line experience.

The Humshaugh C.E. First School's e-Safety policy will operate in conjunction with other policies including those for Information and Communications Technology, Anti-Bullying and the Curriculum. It will be reviewed annually and will be monitored by the Governing body to ensure effective implementation.

End to End e-Safety

e-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-Safety Policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Northumberland Local Authority (LA) including the effective management of filtering packages.
- National Education Network standards and specifications.

Use of the CFE Core e-Safety Policy

This policy has been based upon the Core e-Safety policy which has been approved by the Children, Families and Education Directorate (CFE).

Monitoring

Reports are received quarterly from the Northumberland e-learning and ICT Curriculum Support Team and any incidents are highlighted and followed up by the Headteacher. The procedure to follow after any eSafety incident is available as a flow chart (Appendix D. Attached file: eSaftey_Incident_Flow_Chart.pdf; originally provided on http://ngfl.northumberland.gov.uk/esafe/policy.html)

Further Information

This policy has been updated by Revd. Steve Wilkinson (Governor for esafety) and Jude Long (Headteacher). It will be approved and monitored by the Governing body. For further information, please contact the Governors or Headteacher via the school on 01434 681408 or admin@humshaugh.northumberland.sch.uk

e-Safety Audit

This e-Safety audit can be used to check that all sections of the e-Safety Policy are in place.

The school has an e-Safety Policy that complies with CFE guidance.	Y
Date of latest update: January 2017	
The Policy was agreed by Governors on: 20.1.17	
The Policy is available for Staff in the Policies file.	
The Policy is available for Parents in the Policies file and on the website	
The designated Child Protection Officer is the Headteacher Jude Long	
The e-Safety Coordinator is the Headteacher Jude Long	
All Staff have signed a Staff & Adult Users ICT Acceptable Use Policy.	Y
All Adult Users have signed a Staff & Adult Users ICT Acceptable Use Policy	Y
Rules for Responsible Use have been set for students.	Y
These Rules are displayed in all rooms with computers.	Y
Parents sign and return an agreement that their child will comply with the school Rules for Responsible Internet Use.	Y
A list has been generated of all approved users of the school's Internet.	Y
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y
The school filtering package has been approved by the Headteacher.	Y
An ICT security audit has been initiated by the Headteacher, possibly using external expertise.	Y
School personal data is collected, stored and used according to the principles of the Data Protection Act.	Y
Staff with responsibility for managing filtering and monitoring network access, work within a set of procedures and are supervised by the Headteacher.	Y

Humshaugh C. E. First School
e-Safety Policy

Updated: January 2017

1 Writing and Reviewing

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, Anti-Bullying and the Curriculum.

This e-Safety Policy has been updated by a representative of the Governing body and the Headteacher, using a template provided by Kent County Council www.kenttrustweb.org.uk?esafety as recommended by Northumberland LA.

It was approved by the Governing Body on 20.1.17

The e-Safety Policy will be reviewed annually.

The implementation of the e-Safety policy will be monitored through ongoing Governor visits in accordance with existing practice.

The Headteacher will be responsible for e-Safety in the school.

2 Teaching and Learning

2.1 Why Internet use is important

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience. For example, there will be access to educational resources, museums and art galleries, news and current affairs. There will be opportunities for discussion with experts in many fields, and to communicate and exchange information with students and others worldwide.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- Staff will have the opportunity to access educational materials, to communicate with the advisory and support services, professional associations and colleagues, exchange curriculum and administration data with the Northumberland Local Authority (LA), receive up-to-date information and participate in government initiatives.
- The Internet is used to enhance the school's management information and business administration systems.

2.2 How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;

- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Northumberland LA and DfE;
- access to learning wherever and whenever convenient.

2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- access to learning wherever and whenever convenient.

2.4 How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.

2.5 Using the Internet

- All adult users of the school's computer system (including teachers, supply teachers, classroom assistants, support staff, governors, Out of School Club leaders, Pre-School leaders, Computer Club users and visitors) will be asked to sign the 'Staff & Adult Users ICT Acceptable Use Policy' (Appendix A).
- Access to the Internet will only be granted to pupils once the Rules of Responsible Internet Use (Appendix B) have been discussed and agreed.
- A Parental Consent form is required for each child before access to the Internet is granted (Appendix C)

3 Managing Internet Access

3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly by the Headteacher and improved as and when necessary.
- Virus protection will be updated regularly.
- Security strategies will be reviewed in line with advice from Northumberland LA and the Internet Service Provider (ISP).

3.2 E-mail

- Pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use appropriate to their age.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission from an adult.
- E-mail sent to an external organisation should be written carefully and authorised by an adult before sending, in the same way as a letter written on school headed paper.
- If a pupil receives an offensive e-mail they must immediately close it and inform a teacher.
- The forwarding of chain letters is not permitted.
- Whole -class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Headteacher.

3.3 The School Website

3.3.1 Publishing contact details

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Staff will be referred to by their title and surname unless they request otherwise, and pupils' names will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.3.2 Publishing pupil's images and work

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are electronically published.
- Pupil's work will only be published with the permission of the pupil and parents.

- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

3.4 Social networking and personal publishing

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messenger details and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

3.5 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

3.6 How will filtering be managed?

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with Northumberland LA to ensure that the filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

3.7 How will video conferencing be managed?

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- The equipment must be secure and if necessary locked away when not in use.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the pupils' age and ability.
- Parents and carers consent should be obtained prior to children taking part in video conferences.

3.8 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

4 Policy Decisions

4.1 Authorising Internet access

- All staff and adults users must read and sign the 'Staff & Adult Users ICT Acceptable Use Policy' before using any school ICT resource.
- All pupils will be shown or read the Rules for Responsible Internet Use which will be discussed and agreed before access to the Internet is granted.
- A consent form will be requested from each parent, indicating that they have read and understood the Rules for Responsible Internet Use, have discussed them with their child(ren), and that they give permission for their child(ren) to use the Internet in school.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitor to the school site who require access to the schools network or internet access will be asked to read and sign the 'Staff & Adult Users ICT Acceptable Use Policy'.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- 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.

4.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.) following the eSafety Incident Reporting Flow Chart (Appendix D).
- The Headteacher will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child Protection log.
- The Designated Child Protection Officer will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school discipline/

behaviour policy where appropriate.

- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer.
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other school in Northumberland.

4.4 Handling e-Safety complaints

- If there is an incident in which a pupil is exposed to offensive or upsetting material the school's response will be handled by the e-Safety Co-ordinator, the Child Protection Office and the Headteacher.
- Pupils who are exposed to offensive or upsetting material will be given the appropriate personal support, the pupil's parents/carers will be informed and will be given an explanation of the course of action the school has taken.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

4.5 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-Safety.
- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.
- The school will provide Staff & Adult Users ICT Acceptable Use Policy for any guest who needs to access the school computer system or internet on site.

4.6 Cyberbullying

- Cyberbullying is the use of Information and Communications Technology, particularly mobile phones and the internet, deliberately to upset someone else. 'Upsetting' someone can take a variety of forms. It can involve threatening, distressing or humiliating a target, and, as such, encompasses a wide range of behaviours'. It can mean things like prank calling, sending nasty text messages and posting on hate sites as well as forwarding horrible emails or videos.
- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated.
- All incidents or allegations of cyberbullying reported to the school from any source will be recorded and followed up in line with the eSafety Incident Reporting Flow Chart (Appendix D), and the School's Anti-bullying policy.
- Reassurance and support will be given to those being bullied and those reporting the incident.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be asked to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

4.7 How will Learning Platforms be managed?

- SLT and staff will regularly monitor the usage of the LP by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

4.8 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school ICT Acceptable Use policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

4.9 Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released at the end of the day.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

4.10 Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity, except in an emergency situation as authorised by the headteacher.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by the Headteacher in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Headteacher.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

5 Communications Policy

5.1 Introducing the e-Safety policy to pupils

- e-Safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme is established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.

5.2 Staff and the e-Safety policy

- All staff and adults users must read and sign the 'Staff & Adult Users Code of Conduct' before using any school ICT resource.
- The e–Safety Policy will be formally provided to and discussed with all members of staff
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

5.3 Enlisting parents' support

- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents' attention will be drawn to the School e-Safety Policy by letter initially, and future updates by newsletters, in the school brochure and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged.

Humshaugh C. E. First School
Staff ICT Acceptable Use Policy 2017

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the eSafety policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to the headteacher as Designated Child Protection Coordinator and the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the headteacher.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the headteacher as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

- I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the headteacher.

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

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree with the e-Safety Staff & Adult Users Code of Conduct.

Signed: …… Date: ……

Print: …….. …….. …… Role:……

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 only use websites that an adult has opened for us.

We can click on the buttons or links only when we know what they do.

We immediately close any web page we are not sure about.

We tell an adult immediately if we see anything we are uncomfortable with.

We can send and open e-mails together.

We can write polite and friendly e-mails to people that we know, with the adult who is with us.

Rules for Responsible Internet Use
Key Stage 1
Humshaugh C. E. First School e-Safety Policy, January 2017

Think then Click

These rules help us to stay safe on the Internet

- We ask permission from an adult before using the Internet.
- We only use websites that an adult has chosen, or follow an agreed search plan.
- We immediately close any web page we are not sure about.
- We tell an adult immediately if we see anything we are uncomfortable with.

- We gain permission from an adult before checking the e-mail.
- We do not open e-mails sent by anyone that we don't know.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly and that have been checked by an adult.

- We never give out personal information (including full name, address or telephone numbers) or passwords.
- We never arrange to meet anyone that we don't know.
- We do not use Internet chat rooms or social network spaces.
- We understand that the school may check computer files to monitor Internet sites we visit and e-mails that we send.

Appendix C

Humshaugh C. E. First School
e-Safety Parental Consent Form

The Humshaugh C E First School e-Safety Policy has been updated in order to protect pupils during their use of computer facilities, including access to the Internet, whilst at school. This is an essential part of children's learning, as required by the National Curriculum. All parents are asked to sign and return the form below to show that the following e-Safety Rules, appropriate to the age each child, have been discussed, understood and agreed.

Rules for Responsible Internet Use
Key Stage 1

_ _

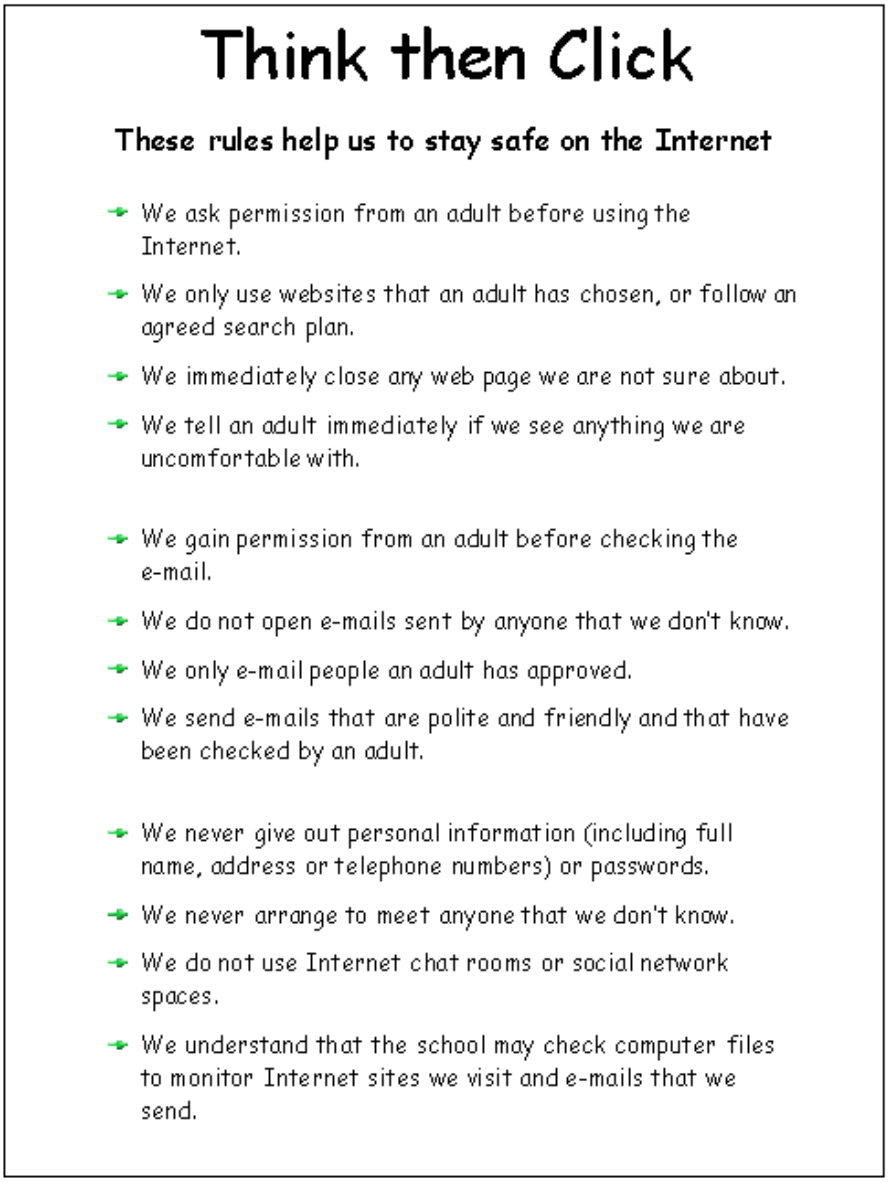
Parental Consent for Internet Access

I have read and understood the school e-Safety Rules for Responsible Internet Use, have discussed them with my child and give permission for my son / daughter to access the Internet in school. 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.

I am aware that the school's e-Safety Policy is available to view upon request from the school.

Signed:	***Parent / Guardian***
Please print name:	***Date:***
Child's name / signature:	

Please sign and return to the School Secretary, Humshaugh C. E. First School.



Rules for Responsible Internet Use
Key Stage 2

Parental Consent for Internet Access

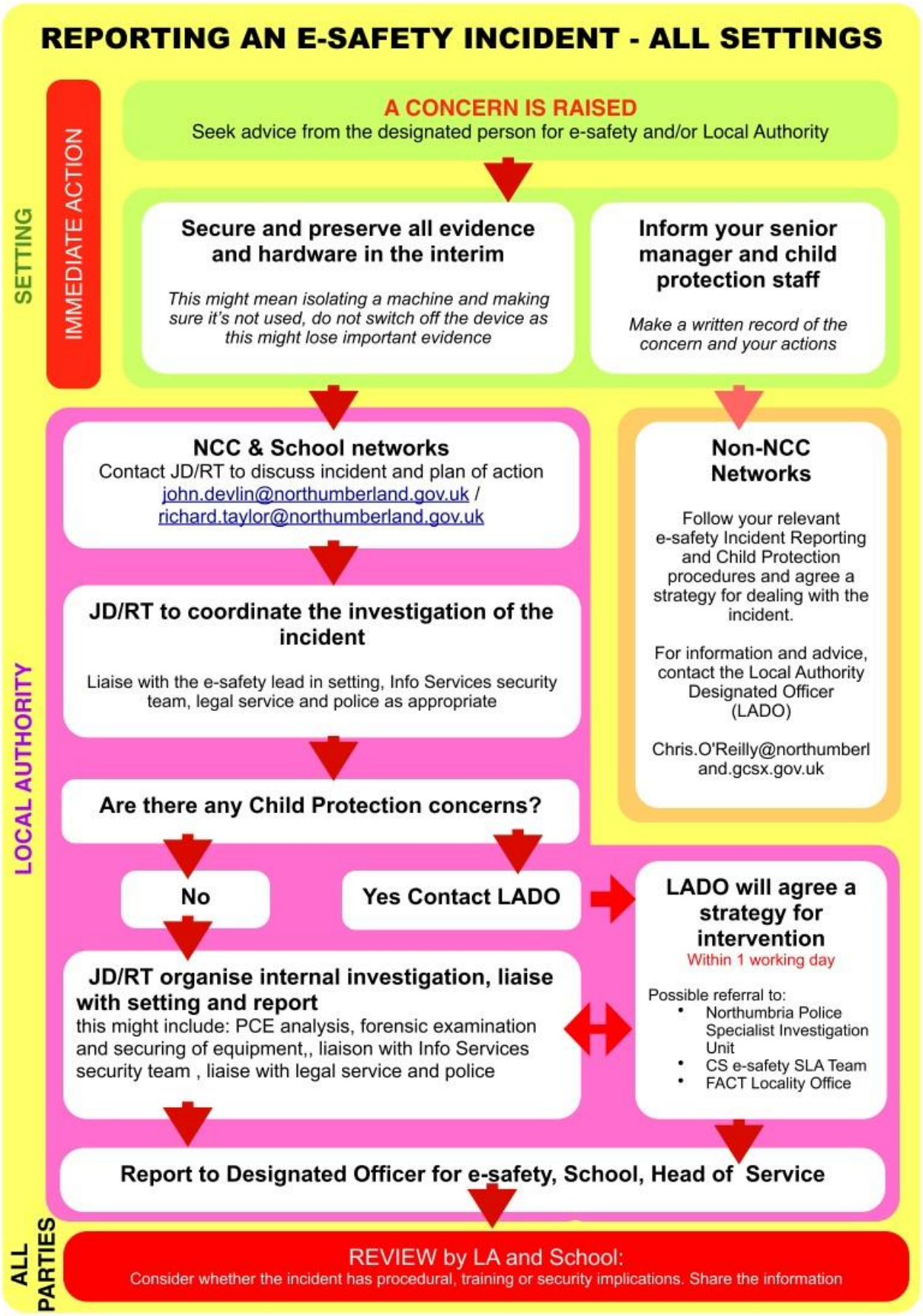
I have read and understood the school e-Safety Rules for Responsible Internet Use, have discussed them with my child and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate 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.

I am aware that the school's e-Safety Policy is available to view upon request from the school.

Signed:	***Parent / Guardian***
Please print name:	***Date:***
Child's name / signature:	

Please sign and return to the School Secretary, Humshaugh C. E. First School.

Appendix D


REPORTING AN E-SAFETY INCIDENT - ALL SETTINGS
SETTING
IMMEDIATE ACTION
A CONCERN IS RAISED
Seek advice from the designated person for e-safety and/or Local Authority
Secure and preserve all evidence and hardware in the interim
This might mean isolating a machine and making sure it's not used, do not switch off the device as this might lose important evidence
Inform your senior manager and child protection staff
Make a written record of the concern and your actions
LOCAL AUTHORITY
NCC & School networks
Contact JD/RT to discuss incident and plan of action
john.devlin@northumberland.gov.uk /
richard.taylor@northumberland.gov.uk
Non-NCC Networks
Follow your relevant e-safety Incident Reporting and Child Protection procedures and agree a strategy for dealing with the incident.
For information and advice, contact the Local Authority Designated Officer (LADO)
Chris.O'Reilly@northumberland.gcsx.gov.uk
JD/RT to coordinate the investigation of the incident
Liaise with the e-safety lead in setting, Info Services security team, legal service and police as appropriate
Are there any Child Protection concerns?
No
Yes Contact LADO
LADO will agree a strategy for intervention
Within 1 working day
Possible referral to:
Northumbria Police Specialist Investigation Unit
CS e-safety SLA Team
FACT Locality Office
JD/RT organise internal investigation, liaise with setting and report
this might include: PCE analysis, forensic examination and securing of equipment,, liaison with Info Services security team , liaise with legal service and police
Report to Designated Officer for e-safety, School, Head of Service
ALL PARTIES
REVIEW by LA and School:
Consider whether the incident has procedural, training or security implications. Share the information