ROTHBURY FIRST SCHOOL

Acceptable Use Policy (Information Technology)

Rothbury First School Acceptable Use Policy (Information Technology)

Date reviewed by Governors:	November 2016
Issued:	January 2017
Date for next review:	November 2017

Pupils Acceptable Use Policy (Information Technology): EYFS, Year 1 and Year 2

- I only use the internet when an adult is with me
- I only click on links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I only send messages online which are polite and friendly
- I know the school can see what I am doing online
- I have read and talked about these rules with my parents/carers
- I always tell an adult/teacher if something online makes me feel unhappy or worried
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online
- I know that I am not allowed to bring devices from home into school (eg: cameras, games consoles, tablets, mobile phones, smart watches) unless this has been agreed beforehand with the Headteacher.
- I know that if I do not follow the rules then there will be consequences in accordance with the school's behaviour policy.

Pupils Acceptable Use Policy (Information Technology): Year 3 and Year 4

- I know that I will be able to use the internet in school, for a variety of reasons, if I use it responsibly. However, I understand that if I do not, I may not be allowed to use the internet at school.
- I know that I am only allowed to use the internet at school during lesson times with permission. I am not allowed to use the internet at other times.
- I know that being responsible means that I should not look for bad language, inappropriate images or violent or unsuitable games, and that if I accidently come across any of these I should report it to a teacher or adult in school or a parent or carer at home.
- I will treat my password like my toothbrush! This means I will not share it with anyone (even my best friend), and I will log off when I have finished using the computer or device.
- I will protect myself by never telling anyone I meet online my address, my telephone number, my school's name or by sending a picture of myself without permission from a teacher or other adult.
- I will never arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- If I get unpleasant, rude or bullying emails or messages I will report them to a teacher or other adult. I will not delete them straight away, but instead, keep them so I can show them to the person I am reporting it to.
- I know that posting anonymous messages or pretending to be someone else is not allowed.
- I will always check with a trusted adult before I download software or data from the internet. I know that information on the internet may not be reliable and it sometimes needs checking.
- I will be polite and sensible when I message people online and I know that sending a message is the same as having a conversation with someone. I will not be rude or hurt someone's feelings online.
- I know that I am not allowed on personal e-mail, social networking sites or instant messaging in school.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online.
- I know that I am not allowed to bring devices from home into school (eg: cameras, games consoles, tablets, mobile phones, smart watches, memory sticks) unless this has been agreed beforehand with the Headteacher.
- I know that if I do not follow the rules then there will be consequences in accordance with the school's behaviour policy.

Technology at Rothbury First School

Dear Parent/Carer

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Your child will have the opportunity to access a wide range of information and communication technology (ICT) resources. This may include access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- School learning platform/intranet
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras
- Recorders and Dictaphones
- Mobile Phones and Smartphones

Rothbury First School recognises the essential and important contribution that technology plays in promoting children's learning and development and offers a fantastic range of positive activities and experiences. However we also recognise there are potential risks involved when using online technology and therefore have developed online e-Safety policies and procedures alongside the schools safeguarding measures.

The school takes responsibility for your child's online safety very seriously and, as such, we ensure that pupils are educated about safe use of technology and will take every reasonable precaution to ensure that pupils cannot access inappropriate materials whilst using school equipment. Access to the web is password controlled and monitored via Northumberland County Council controlled systems. However no system can be guaranteed to be 100% safe and the school cannot be held responsible for the content of materials accessed through the internet and the school is not liable for any damages arising from use of the schools internet and ICT facilities.

Full details of the school's Acceptable Use Policy and e-Safety Policy are available on the school website or on request.

We request that all parents/carers support the schools approach to e-Safety by role modelling safe and positive online behaviour for their child and by discussing online safety with them whenever they access technology at home. Parents/carers can visit the school website's for more information about the school's approach to e-Safety as well as to access useful links to support both you and your child in keeping safe online at home. Parents/carers may also like to visit www.thinkuknow.co.uk, www.childnet.com, www.nspcc.org.uk/onlinesafety, www.saferinternet.org.uk and www.internetmatters.org for more information about keeping children safe online

Whilst the school monitors and manages technology use in school we believe that children themselves have an important role in developing responsible online behaviours. In order to support the school in developing your child's knowledge and understanding about e-Safety, we request that you read the attached Acceptable Use Policy with your child and that you and your child discuss the content and return the attached slip. Hopefully, you will also find this Acceptable Use Policy provides you with an opportunity for conversations between you and your child about safe and appropriate use of the technology, both at school and at home.

Should you wish to discuss the matter further, please do not hesitate to contact the school e-Safety Coordinator, Mrs Cheryl Brotherton, or myself.

Yours sincerely,

Nicki Mathewson

Headteacher

Parent/Carer Acceptable Use Policy (Information Technology) Acknowledgement Form

Pupil Acceptable Use Policy (Information Technology):
Rothbury First School Parental Acknowledgment

I, with my child, have read and discussed the Rothbury First School Pupil Acceptable Use Policy (Information Technology).

I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials however I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet, and that the school is not liable for any damages arising from use of the Internet facilities.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy (Information Technology) or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

I know that my child will receive e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child's Name…….

Class…… Date……..

Parents Name…….....Parents Signature…….

Date……..

Letter for Staff

Dear Colleague

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be "private" and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not accept **either pupils (past or present) or their parents/carers as "friends" on a personal account**. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please only use the office email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this then please speak to the e-Safety Coordinator, Cheryl Brotherton, or to me, the Designated Child Protection Lead.

"Cyberbullying: Supporting School Staff" is available in the staffroom to help you consider how to protect yourself online. Please photocopy them if you want or download the documents directly from www.childnet.com, www.kelsi.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy (Information Technology) and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to the school e-Safety lead, Cheryl Brotherton, or myself if you have any queries or concerns regarding this.

Yours sincerely,

Nicki Mathewson
Headteacher

Rothbury First School

Staff Acceptable Use Policy (Information Technology)

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 school policies, relevant national and local guidance and expectations, and the Law.

Headteacher – Nicki Mathewson

Designated Safeguarding/Child Protection Lead Person – Nicki Mathewson

e-Safety Lead Person – Cheryl Brotherton

ICT Lead Person – Colin Grimes

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

2. 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.

3. 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.

4. I will respect system security and I will not disclose any password or security information and 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 and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Lead Person or the Headteacher.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. 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 that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site will be encrypted by a method approved by the school.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. 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.

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

12. 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 ICT Lead Person as soon as possible.

13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Headteacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. 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.

16. I will promote online 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.

17. 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 e-Safety Lead Person or the Designated Safeguarding Lead Person/Headteacher.

18. 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 and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: …….. Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

Visitor/Volunteer Acceptable Use Policy (Information Technology)

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. 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.

2. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

3. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law.

4. 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.

5. I will promote e-Safety with the children 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.

6. 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 e-Safety Lead Person, Mrs Cheryl Brotherton, or the Headteacher, Mrs Nicki Mathewson.

7. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead Person, Mrs Nicki Mathewson, and/or the e-Safety Lead Person, Mrs Cheryl Brotherton, as soon as possible.

I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.

Signed: …….. Print Name: …….…… Date: …….

Accepted by:……Date: …….