Beeston Rylands Junior School & Trent Vale Infant School

Acceptable Use Policy

September 2018

Review annually
Next review: September 2019

Acceptable Use Policy for Beeston Rylands Junior School and Trent Vale Infant School

1. What is an AUP (Acceptable Use Policy)?

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all on-line technologies (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, mobile phones and games) to safeguard adults and children and young people within the school setting. It details how the school will provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies, beyond the school setting. It also explains procedures for any unacceptable or misuse of these technologies by adults or children and young people.

2. Why have an AUP?

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content that is abusive or pornographic.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst the school or setting acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people are protected.

As part of the Every Child Matters agenda set out by the government, the Education Act 2004 and the Children's Act, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children and young people and parent/carers is also vital to the successful use of on-line technologies, so this policy also aims to inform how parents/carers and children or young people are part of the procedures and how children and young people are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

3. Aims

To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
To outline the roles and responsibilities of everyone within the school setting.
To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

4. Roles and responsibilities of the school:

4.1 Governors and Headteacher

It is the overall responsibility of the Headteacher with the Governors to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated an e-Safety Leader (Rebecca Hollins BRJS; Nicola Beard TVI) to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- Time and resources will be provided for the e-Safety Leader and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the Governors about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors will be made aware of e-Safety developments.
- The Governors **MUST** ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.
- An e-Safety Governor will ensure that the school has an AUP with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including:
    - Challenging the school about having:
        - Firewalls
        - Anti-virus and anti-spyware software
        - Filters
        - Using an accredited ISP (Internet Service Provider)
        - Awareness of wireless technology issues
        - A clear policy on using personal devices.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police or involving parents/carers. See appendices for example procedures on misuse.

4.2 E-Safety Leader

It is the role of the designated e-Safety Leader to:

- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops, IPads and the learning platform. Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Child Protection and ICT leaders so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Decide, in conjunction with the Head teacher, the extent to which the use of personal equipment in school or settings for work purposes (such as digital cameras or the use of a personal e-mail address) is permitted.
- Establish the procedures for using school equipment at home. (The use of personal equipment by staff is disallowed according to the (DfES) DCSF White Paper where there may be communication with children or young people.) It also means all staff members are potentially more at risk of allegations being made against them if using their own equipment, especially if this is unauthorised.

- Home use of school or setting equipment must be in keeping with this policy.
- Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified. Refer to Section 12 of the Allegation Procedure from the LSCBN to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Work alongside the ICT Leader, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that staff have an awareness of how to minimise unsolicited e-mail.

4.3 Staff or adults

It is the responsibility of all adults within the school or other setting to:

- Ensure that they know who the Designated Person for Child Protection is within school or other setting so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher. In the event of an allegation made against the Headteacher, the Chair of Governors must be informed immediately.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Headteacher immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the E-safety Leader.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce this through the curriculum.
- Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within and beyond the school environment, as outlined in appendices.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the e-Safety Leader and ICT Services helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies using the NCC accident/incident reporting procedure in the same way as for other non-physical assaults.

4.4 Children and young people

Children and young people are:

- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time.
- Taught to use the Internet in a safe and responsible manner through ICT, PSHE.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away.

5. Appropriate use by staff or adults

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

5.1 In the event of inappropriate use

If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

6. Appropriate use by children and young people

Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules will be on display wherever there is computer access.

We want our parents/carers to support our rules, which is shown by signing the Acceptable Use Rules so that it is clear to the school or setting, the rules are accepted by the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free in or beyond school.

6.1 In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school or in a setting by not following the Acceptable Use rules, then their parents/ carers will be contacted.

In the event that a child or young person **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action.

7. The curriculum and tools for Learning

7.1 Internet use

- We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PSHE lessons.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that would also be acceptable in 'real life'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

7.2 Video and photographs
The term 'image' refers to the taking of video footage or photographs via any camera or other technology. Images must only be recorded and stored on school equipment.

The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to the school website. Any captions relating to the image must not include details of the child's name. Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. swimming kit. Photographs will be stored on the school server and will either be deleted or archived annually. Images will only be archived for the purposes of monitoring or record keeping.

8. Filtering and safeguarding measures

The broadband connectivity has a filter system which is set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child.

Anti-virus and anti-spyware software is used on all network and stand alone PCs or laptops and is updated on a regular basis.

A firewall (to be included) ensures information about our children and young people and the school cannot be accessed by unauthorised users.

The 'skin' of the on-line personal space is age appropriate and only tools appropriate to the age of the child are to be available.

Links or feeds to e-safety websites are provided.

9. Monitoring
The e-Safety Leader and/or a senior member of staff should be monitoring the use of on-line technologies by children and young people and staff, on a regular basis.
Teachers monitor the use of the Internet during lessons.

10. Computers in shared areas
The computers in the shared areas are protected in line with the school network. Where software is used that requires a child login, it is password protected so that the child is only able to access themselves as a user. Children and young people will be taught not to share passwords.

The same acceptable use rules apply for any staff and children and young people using this technology.

11. Parents
11.1 Roles
Each child or young person will receive a copy of the Acceptable Use Rules on entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.
School will keep a record of the signed forms.

11.2 Support

A list of useful websites that could be used to increase awareness of e-safety will be available to parents/ carers.
The Appendices detail where parents/carers can go for further support beyond the school. The school will endeavour to provide access to the Internet for
parents/carers so that appropriate advice and information can be accessed where there may be no Internet at home, subject to arrangement.

12. Links to other policies:

12.1 Behaviour and Anti-Bullying Policies

12.2 Child Protection Policy

12.3 PSHE

12.4 Health and Safety
12.5 I.C.T.

12.6 Use of images policy

Appendices

Staff Procedures Following Misuse by Staff

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Ensure that no one else can access the material by shutting down.
Log the incident.
Report to the Headteacher and e-Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA/RBC filtering services as with A.

C. An adult receives inappropriate material.
Do not forward this material to anyone else – doing so could be an illegal activity.
Alert the Headteacher immediately.
Ensure the device is removed and log the nature of the material.
Contact relevant authorities for further advice e.g. police.

D. An adult has used ICT equipment inappropriately:
Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately, if necessary.
Report to the Headteacher and Designated Person for Child Protection immediately, who should then follow the Allegations Procedure and Child Protection Policy from Section 12, LSCBN.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Headteacher to implement appropriate sanctions.
If illegal or inappropriate misuse is known, contact the Headteacher or Chair of Governors (if allegation is made against the Headteacher) and Designated Person for Child Protection immediately and follow the Allegations procedure and Child Protection Policy.
Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website (or printed out) about an adult in school:
Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk filtering service for school and LA/RBC so that it can be added to the banned list or use Local Control to alter within your setting.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform LA/RBC as above.

C. A child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Headteacher and Designated Person for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Headteacher must follow the Allegation Procedure and/or Child Protection Policy from Section 12, LSCBN.
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or about a child in school:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the RBC/LA/LSCBN and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.
To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies that will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Learning Platform (Fronter) whilst on the school premises
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Headteacher, Designated Person for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person for Child Protection is.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Headteacher and/or e-Safety Leader.
- I know that I should complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and agree with these Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed……Date…….
Name (printed)……
School……..

e-Safety Acceptable Use Rules Letter to Parents/Carer

BRJS How to be a good digital Citizen:

Our e-safety code: Zip it, block it, flag it.

This code reminds us of our e-safety rules and the actions the children should take if any rules are broken.

Our rules:

Communicate in a kind way

Let an adult know if something worries you

I search responsibly on the internet

Check the information is reliable

Keep personal details to yourself

Name:_____ Signed _____ Date_____

Trent Vale Infant and Nursery School and Beeston Rylands Junior School

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet.

In order to support the school in educating your child about the acceptable use of ICT equipment including the safe use of the Internet (e-Safety), please read the following rules with your child then sign and return the slip.

In the event of a breach of the Rules by any child or young person, the Acceptable Use policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school.

Should you wish to discuss the matter further please contact the Headteacher.

Yours faithfully,

Head teacher

Acceptable Use Rules Return Slip

- I have read and discussed the Rules and confirm that I understand what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Name of Child: _____

Parent/Carer Signature: _____ Date: _____

Trent Vale Infant and Nursery School

These are our rules for using the Internet safely.

Our Internet Rules

Key Stage 1

We talk the children through these rules each time we use the internet.

- **People you don't know are strangers. They're not always who they say they are.**
- **Be nice to people on the computer like you would in the playground.**
- **Keep your personal information private.**
- **If you ever get that "uh oh" feeling, you should tell a grown up you trust.**

Foundation Stage

- **Be nice to people on the computer like you would in the playground.**
- **If you ever get that "uh oh" feeling, you should tell a grown up you trust.**

Useful websites

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)
- www.nen.org.uk (for schools and settings – access to the National Education Network)