Northamptonshire Local Safeguarding Children Board

Acceptable Use Policy

Sub Committee Reviewed (date) May 2018	Signed (Headteacher) *Sarah Dugdale*
Full Governing Body Ratified (date) May 2018	Signed (Chair of Governors) *Cei Davies Linn*
Review Date	*July 2020*

Northamptonshire County Council

CONTENTS

What is an Acceptable Use Policy (AUP)?

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within a school or other educational setting. The policy recognises the ever changing nature of emerging technologies and highlights the need for regular review to incorporate development within Computing. At present the internet technologies used extensively by young people in both home and school environments include:

- Websites
- Social Networking and Chat Rooms
- Gaming
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Learning Platforms
- Video Broadcasting

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. The policy should also 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 or educational setting. It explains procedures for any unacceptable use of these technologies by adults, children or young people.

Why have an Acceptable Use Policy?

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 access these technologies.

The 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.
- Sexting - the sending of indecent personal images, videos or text via mobile phones for private viewing. Can potentially be widely distributed and publicly viewed.
- On-line content which 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 should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children and young people continue to be protected.

As part of the Keeping Children Safe in Education (Sept 2016) 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, young people and parent/carers

is also vital to the successful use of on-line technologies. This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also informs as to how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

1 Aims

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

2 Roles and responsibilities of the school

2.1 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 as designated e-Safety Leader implements agreed policies, procedures, staff training, curriculum requirements and takes the lead responsibility for ensuring e-Safety is addressed in order to establish a safe Computing learning environment. All staff and students are aware of who holds this post within the school.
- Time and resources should 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 should inform the Governors at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or Computing) and ensure Governors know how this relates to child protection. At the Full Governor meetings, all Governors are to be made aware of e-Safety developments from the Curriculum meetings.
- 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 (can be the ICT or Child Protection Governor) ought to challenge the school about having an Acceptable Use Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using Computing, 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
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures (see the Allegation Procedure – Section 12 of Northamptonshire and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers. See appendices for example procedures on misuse.

2.2 e-Safety Leader

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

- Appreciate the importance of e-safety within school and to recognise that all educational establishments have a general duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe Computing learning environment within the school.
- Ensure that the Acceptable Use Policy 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, children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report any issues arising to the relevant governing body sub committees.
- Liaise with the PSHE, Child Protection and Computing leads 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.
- Transparent monitoring of the internet and on-line technologies.
- 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 NCSB to ensure the correct procedures are used with incidents of misuse (website in Appendices).
- Work alongside the Computing Co-ordinator, to ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, standalone 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, standalone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to section 12 of the Allegation Procedure, Northampton Children's Safeguarding Board, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails.

2.3 Staff or adults

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

- Ensure that they know who the Designated Persons for Child Protection are 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, who should then follow the whistleblowing policy.
- 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 technologies so that they know how to use them in a safe and responsible manner. Children and young people should 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 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 General Data Protection Regulations (GDPR May 2018). 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. School Business Manager/Bursars will need to ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the e-Safety Leader and Easipc 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 or memory stick when transferring information from the internet on a regular basis, especially when not connected to the school/educational setting's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information are encrypted or password protected in the event of loss or theft.
- 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.

2.4 Children and young people

Children and young people should be:

- Involved in the review of Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.
- 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 Computing, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

3. Appropriate and Inappropriate Use

3.1 By staff of adults

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

The Headteacher has 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 should 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.

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.

3.2 By Children or Young People

Acceptable Use Rules and the letter for children, young people and parents/carers are outlined in the Appendices. These detail how children and young people are expected to use the internet and other technologies within school or other settings, including 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.

Schools or educational settings should encourage parents/carers to support the rules with their child or young person. This can be shown by signing the Acceptable Use Rules together so that it is clear to the school or setting that the rules are accepted by the child or young person with the support of 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.
Further to this, it is hoped that parents/carers will add to future rule amendments or updates to ensure that they are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

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.

The school council are actively involved in discussing the acceptable use of technologies and the rules for misusing them.

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, the following consequences should occur:

- Any child found to be misusing the internet by not following the Acceptable Use Rules may have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules may result in not being allowed to access the internet for a period of time and another letter will be sent home to parents/carers.

- A letter may be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.

4 The curriculum and tools for Learning

4.1 Internet use

Schools and educational settings should teach children and young people how to use the internet safely and responsibly. They should also be taught, through Computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning.
A range of published schemes are used to teach internet and E-mail lessons from Years 1 onwards. e-Safety lessons and resources can also be found at www.thinkuknow.co.uk for KS1.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

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

- 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.

4.2 Pupils with additional learning needs

The school or setting should strive to provide access to a broad and balanced curriculum for all learners and recognise the importance of tailoring activities to suit the educational needs of each pupil. Where a student has specific learning requirements, or poor social understanding, careful consideration is given to the planning and delivery of e-safety awareness sessions and internet access.

4.3 E-mail use

The school may have email addresses for children and young people to use, as a class as part of their entitlement to being able to understand different ways of communicating and using Computing to share and present information in different forms.

4.4 Mobile phones and other emerging technologies

(i) Personal mobile devices

Staff should be allowed to bring in personal mobile phones or devices for their own use, but **must not use personal numbers to contact children and young people under any circumstances.**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras (see 7.6 for further details)
- Staff should be aware that games consoles such as the Sony Playstation, Microsoft Xbox and other such systems have Internet access which may not include filtering. Before use within school, authorisation should be sought from the Headteacher and the activity supervised by a member of staff at all times.
- The school is not responsible for any theft, loss or damage of any personal mobile device.

(ii) School/educational establishment issued mobile devices

The management of the use of these devices should be similar to those stated above, but with the following additions:

- Where the establishment has provided a mobile device to a member of staff, such as a laptop or mobile phone, only this equipment should be used to conduct school business outside of the school environment.

It should also be policy to ensure that children and young people understand the use of a public domain and the consequences of misuse. Relevant curriculum links should be made to highlight the legal implications and the involvement of law enforcement. Other technologies which schools and settings use with children and young people include:

. photocopiers
. fax machines
. telephones

4.5 Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to cameras, mobile phone, video, interactive whiteboards and visualisers.

It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although Child Protection Guidance states either a child's name or a photograph but not both.

Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit. Photographs are stored on the shared area and will only be used within school. Photographs will remain on the system up to three years.

5 Managing Social Networking and other Web 2.0 technologies

5.1 Social networking advice for staff

Social networking outside of work hours, on non school-issue equipment, is the personal choice of all school staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with pupils such as private email address, telephone number or home address. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Headteacher authorised systems.
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invites from colleagues until they have checked with them in person that the invite is genuine (avoiding fake profiles set up by students).

6. Safeguarding measures

6.1 Filtering

Staff, children and young people are required to use the personalised learning space and all tools within it, in an acceptable way.
Please refer to the Acceptable Use Rules for Staff and children and young people for the appropriate use of the learning platform.

The Exa broadband connectivity has a filter system which should be set at an age appropriate level so that inappropriate content is filtered and tools are appropriate to the age of the child. **All** filtering should be set to 'No Access' within any setting and then controlled via:

- Portal Control (controls filtering at local site level) which controls individual access to the Internet.
- Local Control – controls access to websites and provides the option to add to a 'restricted list'.

The Headteacher should agree to the filtering levels being maintained as part of the connectivity to broadband requirements from Exa. The minimum of Becta Level Four should be met. The levels listed below are in relation to age-appropriate categories:

The filtering complies with the agreed connectivity legalities with Exa and also ensures our younger audiences are not exposed to unnecessary risks.
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 ensures information about children and young people and the school cannot be accessed by unauthorised users.

Children should use a search engine that is age appropriate such as AskJeeveskids or Yahooligans.

6.2 Tools for bypassing filtering

Web proxies are probably the most popular and successful ways for pupils to bypass internet filters today, identifying a cause for concern amongst schools and educational settings where children and young people can access the internet. Web proxies provide an anonymous route through filtering safeguards in existence on networked facilities, allowing users to navigate through potentially harmful or inappropriate content. A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which material can be viewed. The most common use of this tool amongst students is to access social networking features, gaming websites or

information of an adult nature- all of which is blocked through the school or educational establishment's filtering system.

Pupils and staff are forbidden to use any technology designed to circumvent, avoid or bypass any school or educational setting's security controls (including internet filters, antivirus solutions or firewalls.) as stated in the Acceptable Use Rules.
Violation of this rule should result in disciplinary or in some circumstances legal action. Please refer to the 'Staff Procedures Following Misuse by Staff/Children and Young People' sections of this document.

7. Monitoring

The e-Safety Leader should be monitoring the use of on-line technologies by children and young people and staff, on a regular basis.
Network Managers should not have overall control of network monitoring.
Teachers should monitor the use of the learning platform and internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.

8. Parents

8.1 Roles

Each child or young person will receive a copy of the Acceptable Use Rules on first-time entry to the school which will need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.
It should be expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.
School should keep a record of the signed forms.

8.2 Support

As part of the approach to developing e-safety awareness with children and young people, the school or setting may offer parents the opportunity to find out more about how they can support the school or setting in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school. The school or setting may want to promote a positive attitude to using the World Wide Web and therefore want parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly.
Schools should hold Parent/Carer Information Evenings once per annum.
Use the Childnet International 'KnowITAll for Parents' on-line materials to deliver key messages and raise awareness for parents/carers and the community. Ensure that skills around internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using. Part of this evening will provide parents with information on how the school protects children and young people whilst using the learning platform facilities, such as the internet and E-mail. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible internet users and how this can be extended to use beyond the school environment.
The appendices detail where parents/carers can go for further support beyond the school. The school should 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.

9. Links to other policies

9.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. People should not treat on-line behaviours differently to off-line behaviours and should have exactly

the same expectations for appropriate behaviour. This is a key message which should be reflected within Behaviour and Anti-bullying Policies as it is only the tools and technologies that change, not the behaviour of children, young people and adults.

9.2 Managing allegations and concerns of abuse made against people who work with children.

For referrals regarding adults in education; designated officers (formally LADO) 01604 364013.
Email: LADOReferral@northamptonshire.gcsx.gov.uk
Allegations made against a member of staff should be reported to the designated person for child protection within the school or educational setting immediately. In the event of an allegation being made against a Headteacher, the Chair of Governors should be notified immediately.
All allegations made against staff will be reported to the LADO.

9.3 PSHE

The teaching and learning of e-Safety should be embedded within the PSHE curriculum to ensure that the key safety messages about engaging with people are the same whether children and young people are on or off line.

9.4 Health and Safety

Refer to the Health and Safety Policy and procedures of the school/setting and the County Council for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

9.5 School website

The uploading of images to the school website should be subject to the same acceptable rules as uploading to any personal on-line space. Permission ought to be sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

9.6 Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

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 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 e-Safety Leader immediately.
Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
Inform the LA 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, NCSB.
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 about an adult in school:**
Preserve any evidence.
Inform the Headteacher immediately and follow Child Protection Policy as necessary.
Inform the RBC/LA/NCSB and eSafety 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 eSafety 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. **An adult or 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, NCSB.
Contact CEOP (police) as necessary.

D. **Threatening or malicious comments are posted to the school website about a child in school**:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the RBC/LA/NCSB 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.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.
If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

Procedures need to be followed by the school within Section 12 of the Allegations Procedure and Child Protection Policy from the Local Safeguarding Children's Board Northamptonshire guidance.
All adults should know who the Designated Person for Child Protection is.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Northamptonshire County Council

Acceptable Use Rules for Staff, Governors and Visitors

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 which 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 internet or send them via E-mail.
- 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 (e-Safety Leader) or Designated Person for Child Protection 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.
- 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 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 will adhere to copyright and intellectual property rights.
- I will only install hardware and software I have been given permission for.
- I accept that the use of any technology designed to avoid or bypass school filtering systems is forbidden. I understand that intentional violation of this rule may result in disciplinary procedures for staff misuse.
- 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 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 for Primary

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the internet, E-mail and personal on-line space via Exa.

In order to support the school in educating your child/young person about e-Safety (safe use of the internet), please read the following Rules with your child/young person then sign and return the slip.

In the event of a breach of the Rules by any child or young person, the e-Safety 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/young person about safe and appropriate use of the internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

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

Yours faithfully,

Sarah Dugdale
Headteacher

---

e-Safety Acceptable Use Rules Return Slip

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood 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.

Parent/Carer Signature: _____ Date: _____

Key Stage 1

These are our rules for using the internet safely.

Our Internet and E-mail Rules

- We use the internet safely to help us learn.
- We learn how to use the internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password a secret.
- We know who to ask for help.
- If we see something we do not like we know what to do.
- We know that it is important to follow the rules.
- We are able to look after each other by using our safe internet.
- We can go to www.thinkuknow.co.uk for help.

Further Information and Guidance

The nature of e-safety is evolving. Encourage safe practice. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- 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.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)
- http://www3.northamptonshire.gov.uk/NACPC/Adults (Local Safeguarding Children's Board Northamptonshire – policies, procedures and practices, including Section 12 of the Allegations Procedures are available here)
- www.nen.org.uk (for schools and settings – access to the National Education Network)
- https://enable.lpplus.net/ht/e-Safetyhome (for schools and settings to access e-Safety guidance and support)

Author	Sarah Dugdale
Sub Committee Reviewed (date)	Signed (Headteacher)
Full Governing Body Ratified (date)	Signed (Chair of Governors)
Review Date:	*May 2020*