Grendon CE Primary School

Acceptable Use Policy (incorporating E-safety)

This policy is has been adapted from the Northamptonshire Acceptable Use Policy which was designed for use by Headteachers, Governors, e-Safety Leaders and the Designated Person for Child Protection.

This Policy should be used in conjunction with the Child Protection Policy, the Health and Safety Policy, the Anti-Bullying Policy and the ICT curriculum policy.

This policy was originally drafted by N.C.C. as a guide for **all schools and educational settings**, where many e-safety risks and management issues are the same, with the same key messages for children, young people, their parents/carers and staff/other users.

The content has been adapted to the needs and curriculum of our children and young people whilst still reflecting the key messages and procedures required to successfully implement the N.C.C. requirements.

Using the EMBC and Enable broadband services as outlined in this policy will ensure our school meets the requirements for safeguarding on-line users.

This policy has been developed by the Children and Young People's Service in consultation with Education Welfare - CYPS, Northamptonshire Police, the Local Safeguarding Children's Board Northamptonshire, Governors and Parents/Carers and Children.

Northamptonshire County Council

police

LOCAL SAFEGUARDING CHILDREN BOARD NORTHAMPTONSHIRE

Northamptonshire County Council Acceptable Use Policy for Schools

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 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 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 continued to be 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.
•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 (or establishment):

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 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 through the Curriculum and Pupil Welfare Sub-Committee 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 meetings of the Full Governing Body, all Governors will 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) will challenge the school about having 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 (see the Allegation Procedure – Section 12 of Local Safeguarding Children's Board Northamptonshire) and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via our agreed protocols with 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 (HT) 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 and the learning platform *or* ensure the technician is informed and carries out work as directed.
- 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 which should then be fed into the Curriculum and Pupil Welfare sub-committee.
- Liaise with the PSHE, Child Protection and ICT 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
- Decide the use of personal equipment in school or settings for work purposes, such as a digital camera or the use of a personal e-mail address and the procedures for using school equipment at home – signed acceptable use forms by staff need to be considered if using own equipment so that it is clear how, when, why and where equipment is used and storing/discarding of images etc…takes place.
- 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 unsolicited e-mails to a member of staff from other sources is minimised. Refer to section 12 of the Allegation Procedure, LSCBN, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication
      (To be reviewed in light of union consultation according to workforce agreements.)
- Report overuse of blanket e-mails or inappropriate tones to the Headteacher and/or Governors.

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, who should then follow the Allegations Procedure, Section 12, LSCBN, where appropriate.

- 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 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.
  School 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 Synetrix helpdesk in order that inappropriate sites are added to the restricted list or control this with the Local Control options via your broadband connection (through Community Gateway).

- 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:
- Involved in the review of our Acceptable Use Rules through the school council 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 ICT, 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).

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. Staff training should underpin the receipt of this policy.

When accessing the Learning Platform from home, the same Acceptable Use Rules will apply. The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.
Please refer to appendices for a complete list of Acceptable Rules for Staff.

5.1 In the event of inappropriate use
If a member of staff is believed to misuse the Internet or learning platform (enable or Community Gateway) in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations Procedure (Section 12, LSCBN) 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 within the classrooms.

We want our parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, 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, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules 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. File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using the learning platform (Enable) 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 the following consequences will occur (these will be reviewed by our school council and stakeholders as the policy is updated):

- Any child found to be misusing the Internet by not following the Acceptable Use Rules will 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 will 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 will 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.

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, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.

Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

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 where the following concepts, skills and competencies have been taught by the time they leave Year 6:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

We use the NIAS Scheme of Work for ICT to teach Internet and E-mail lessons from Years 1 to 6, where each unit of work contains a lesson on e-safety or we use the www.thinkuknow.co.uk resources for KS1 and KS2, within PSHE.

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 will 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 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 Learning Platform (Enable)
The Northants learning platform (Enable) provides a wealth of opportunity for adults, children and young people within and beyond school to:

- access resources via the National Education Network (NEN) which extends regionally to support schools
- collaborate and share work via web cams and uploading
- ask questions
- debate issues
- dialogue with peers
- dialogue with family members or carers
- access resources in real time
- access other people and cultures in real time
- develop an on-line community

The tools available for use within the learning platform (Enable) for adults, children and young people include:

- Internet access
- E-mail
- Video-conferencing
- Weblogs (on-line diaries)

- Wikis (on-line encyclopaedia or dictionary)
- Instant Messaging
- An on-line personal space for adapting as a user to:
    - upload work
    - access calendars and diaries
    - blog

The personal space (My Site) contains some information about the user. This area should be used as an opportunity to discuss with children and young people appropriate information to enter to **ANY** website asking for personal details (such as a social networking site e.g. Bebo and Facebook) and should reflect key messages for any on-line use.

Children and young people should use their login and password to access the Internet via the learning platform (Enable) so that the level of filtering is appropriate. Staff should be ensuring that children and young people are not bypassing the login to the Community Gateway (broadband connection) to get to Enable so that they are protected to the best of the school's ability, in line with the Embc-pl AUP and NCC policy.

Staff or adults need to ensure they consider the risks and consequences of anything they or their children and young people may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

7.3 E-mail use
We have E-mail addresses for children and young people to use, as a class and/or as individuals, as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms. Individual E-mail accounts can be traced if there is an incident of misuse.

Staff, children and young people are to use their school issued e-mail addresses for any communication between home and school only. A breach of this will be considered a misuse and will result in consequences.

Parents/carers are encouraged to be involved with the monitoring of E-mails sent although the best approach with children and young people is to communicate about who they may be talking to and assess risks together.

Teachers are expected to monitor their class use of E-mails where there are communications between home and school/setting, on a regular basis. Where an establishment has a network manager, there is an expectation that monitoring software is used to flag up inappropriate terms and that a Senior Member of the Team has an overview of potential issues on a regular basis – refer to the Monitoring section for further information.

7.4 Video-conferencing
The use of web cams to video-conference will be via Enable which is a filtered service.
Children need to ask for permission from a member of staff or adult to use this facility both in and beyond school.
Children need to tell an adult immediately of any inappropriate use by another child or adult (This is part of the Acceptable Use Rules.)

Where children and young people (and adults) may be using a web cam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Rules.

Taking images via a web cam will follow the same procedures as taking images with a digital or video camera.

7.5 Mobile phones and other technologies
Schools and settings should carefully consider how the use of mobile technologies can be used as a teaching and learning tool within the curriculum, with the following areas of concern to be taken into consideration:

- inappropriate or bullying text messages
- images or video taken of adults or peers without permission being sought
- 'happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult which is often distributed

Further guidance from the DCSF around the misuse of these technologies can be found at www.teachernet.gov.uk/publications

The use of mobile phones is not allowed in our school by children. Staff are permitted to use their mobile phones in school at times when they are not working with children. This also applies to other mobile technologies such as PDAs. Children may use their mobile phones at events such as School discos or games evenings. The same rules of acceptable use will apply to mobile phone users at these times.

Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances.

It is also our policy to ensure that we educate our children and young people in understanding the use of a public domain and the consequences of misusing it including the legal implications and law enforcement through relevant curriculum links.

Other technologies schools and settings use with children and young people are:

- *photocopiers*
- *fax machines*
- *telephones*
- *PDAs*
- *Laptops*

7.6 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.

In our school, it is considered inappropriate for any staff to use their personal equipment including cameras and mobile phones to take pictures of children. This decision has been taken as it can leave staff in vulnerable positions if they have images of children on their personal cameras and phones. There are cameras designated to each class and sufficient surplus cameras available in school for visits or specific curriculum days.

The personal space (My Site) on the Enable learning platform should not have personal photographs uploaded that reveal more than a general location, an activity (without close-ups of children's or young person's faces) or piece of work, without the express permission of parents/carers and school or setting. It is also highly recommended that permission is sought prior to any uploading of images to check for inappropriate content.

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.

Photographs/images used to identify children and young people in a forum or using Instant Messaging within enable will be representative of the child rather than of the child e.g. an avatar.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a 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. School will need to decide how photographs will be used, including where they will be stored (central location which could be viewed by anyone) and when they will be deleted.

8. Filtering and safeguarding measures

Staff, children and young people are required to use the personalised learning space (Enable) 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 RM Broadband 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.

The Enable learning platform is set within a filtering service that will provide the same level of protection for all users.

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.

An RSS (Really Simple Syndication) feed provides a direct link to commonly used websites so that children and young people do not need to leave their personal space for updates.

Links or feeds to e-safety websites are provided.

For older children and young people, the Report Abuse button is available should there be a concern of inappropriate or malicious contact made by
someone unknown. This provides a safe place for children and young people to report an incident if they feel they cannot talk to a known adult.

CEOP (Child Exploitation and On-line Protection Centre) training for secondary children and young people (and Year 6 Primary children) is annual and part of the PSHE curriculum for raising awareness on staying safe and being responsible. A link to the www.thinkukknow.co.uk website is part of the skin layout for further advice and information on children's or young people's personal on-line spaces.

Encryption codes on wireless systems prevent hacking.

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.

Network Managers should not have overall control of network monitoring.

Teachers monitor the use of Enable and the Internet during lessons and also monitor the use of e-mails from school and at home, on a regular basis.

10. School library

The computers in the school library 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 should 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

(There is no statutory requirement for parents to sign acceptable use policies but evidence shows that children and young people signing agreements to take responsibility for their own actions, is successful.
http://www.teachers.tv/video/22517 shows an excellent example of this for bullying.)

Each child or young person will receive a copy of the Acceptable Use Rules on an annual basis or first-time 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

Schools and settings may choose to follow or adapt this guidance:
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.

We will hold Parent/Carer Information Evenings bi-annually and use the Childnet International 'KnowITAll for Parents' CD/on-line materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community. 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 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

Please refer to the Behaviour and Anti-Bullying Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. Schools should have an up to date Anti-bullying Policy which will include any cyberbullying issues. *All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and young people and their parents/carers.* 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.

12.2 Allegation Procedures and the Child Protection Policy
Please refer to the Allegation Procedure, Section 12, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Headteacher immediately or Chair of Governors in the event of the allegation made about the Headteacher.

The (DfES) DCFS White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people and young people about homework or any other school issues either in or beyond school and any such action should be dealt with.
We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.

Please refer to the Child Protection Policy (Section 12 LSCBN) for the correct procedure in the event of a breach of child safety and inform the designated person for child protection within school immediately.

12.3 PSHE
We link the teaching and learning of e-Safety with our PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people.

12.4 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.

12.5 School website
The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission is always 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.

12.6 External websites
In the event that a member of staff finds themselves or another adult on an external website, such as 'Rate My Teacher', as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

12.7 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/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 learning platform (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.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, LSCBN.
Contact CEOP (police) as necessary.

D.Threatening or malicious comments are posted to the school website or learning platform 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.

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.

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 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, 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 for Primary or Secondary

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet, E-mail and personal on-line space via the East Midlands Broadband Consortium (embc).

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 me via the school office.

Yours faithfully,

John Wayland
Headteacher

e-Safety Acceptable Use Rules Return Slip, 2010 – 2011

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.

Key Stage 2

These are our rules for using the Internet safely and responsibly.

Our On-line Rules
• We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly. • We send e-mails and messages that are polite and friendly. • We will only e-mail, chat to or video-conference people an adult has approved. • Adults are aware when we use on-line tools, such as video-conferencing. • We never give out passwords or personal information (like our surname, address or phone number). • We never post photographs or video clips without permission and never include names with photographs. • If we need help we know who to ask. • If we see anything on the Internet or in an e-mail that makes us uncomfortable, we know what to do. • If we receive a message sent by someone we don't know we know what to do. • We know we should follow the rules as part of the agreement with our parent/carer. • We are able to look after each other by using our safe Internet in a responsible way. • We know that 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.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)
- http://www.northamptonshire.gov.uk/NACPC/acpc_home.htm (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://northants.lpplus.net (for schools and settings to access the Northants Learning Platform – click on the e-Safety tab for up-to-date information)