NORTHAMPTON PRIMARY
ACADEMY TRUST PARTNERSHIP

Acceptable Use Policy: Incorporating E-Safety

Date approved by the NPAT Board of Directors:	13 December 2018
Chair of Directors Signature:	
Renewal Date:	September 2021

The e-Safety Lead for Headlands Primary School **is:** Mr Deane Kelly

The Designated Persons for Child Protection are: Mr Darren Smith, Mrs Karen Smith, Mrs Sharon Ritchie

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

This 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 our school. The policy recognises the everchanging nature of emerging technologies within the curriculum and media and highlights the need for regular review to incorporate development within ICT. At present the internet technologies used extensively by young people in both home and school environments include:

- School websites/blogs
- Social Networking
- Gaming/forums on Xbox live etc.
- Music Downloading
- Mobile phones with wireless connectivity
- Email and Instant Messaging
- Office 365
- Skype
- Video Broadcasting
- Apple/Windows apps

This policy provides 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 also explains procedures for any unacceptable use of these technologies by children or young people and refers to school disciplinary procedures for staff.

2. Why have an AUP?

The use of the internet as a tool to communicate and 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:

- Spam and other inappropriate e-mail
- Online grooming
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device
- Viruses
- Cyberbullying
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing
- On-line content which is abusive or pornographic
- Radicalisation and other religious movements
- Social and emotional effects of an increased use of technology

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. Where possible, another member of staff should be copied into emails to also reduce risks. There is also a responsibility to educate parents about the risks and how this is managed inside school, along with what they can do at home to help safeguard their child.

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. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure children and young people continue to be protected.

3. 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, including parents, 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.

4. Responsibilities of the school

4.1 Headteacher and Governors

The Headteacher and Governors have overall responsibility for e-Safety as part of the wider remit of safeguarding and child protection. To meet these responsibilities, the following measures are in place:

- The Headteacher has designated an e-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed appropriately. All staff and students are aware of who holds this post within the school.
- Time and resources are provided for the e-Safety Lead and staff to be trained and update policies, where appropriate.
- The Headteacher promotes e-Safety across the curriculum and has an awareness of how this is being developed and linked with the school development plan.
- The Headteacher will inform the Governors at all meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure they know how this relates to child protection.
- The Governors must ensure that e-Safety is embedded within all Child Protection training, guidance and practices.
- An e-Safety Governor (who may in many cases also be the nominated Safeguarding Governor) has been elected to challenge the school about: ○ Firewalls
  - Anti-virus and anti-spyware software ○ Filters
  - Using an accredited ISP (Internet Service Provider) ○ Awareness of wireless technology issues ○ Clear policies on using personal devices
  - Procedures for misuse, allegations or dealing with e-Safety incidents

4.2 e-Safety Lead

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

- Recognise the importance of e-safety and understand the school's duty of care to ensure the safety of their pupils and staff.
- Establish and maintain a safe ICT learning environment within the school.
- Update the AUP annually and share it with staff and parents where appropriate.
- Ensure that filtering is set to the correct level for staff, children and young people accessing school equipment, or ensure that the technician is informed and carries out work as directed.
- Ensure that all adults understand how filtering levels operate and their purpose.
- Report issues and update the Headteacher on a regular basis.

- Liaise with the PSHE, Child Protection and ICT leads so that policies and procedures are updated and take into account any emerging issues and technologies.
- Co-ordinate or deliver staff training according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Make staff aware of the LSCBN Safeguarding Procedures at www.proceduresonline.com/northamptonshire/scb/
- Implement a system of monitoring staff and pupil use of school issued technologies and the internet, where appropriate. This will be done by monitoring issues when concerns are raised.
- Maintain an e-Safety Incident Log, to be shared with the Headteacher and Governors at agreed intervals.
- Train staff on how to log an e-Safety incident.
- Ensure that anti-virus software and anti-spyware is updated on the network, PCs and teacher/child laptops and that this is reviewed on a regular basis.
- Oversee monitoring of internal emails, where:
    - Blanket e-mails are discouraged
    - Tone of e-mails is in keeping with all other methods of communication

Look at and monitor how E-Safety is taught throughout KS1 and KS2 to ensure coverage in line with the government and OFSTED guidance.

4.3 Staff

It is the responsibility of all adults within the school to:

- Know who the Designated Person for Child Protection is, so that any misuse or incidents involving a child can be reported. Please refer to chapter on Managing Allegations Against Staff for further details.
- Be familiar with, or know where to access school policies, including Child Protection, Anti-bullying, Disciplinary Procedures and Codes of Conduct.
- Check the filtering levels are appropriate for their students and are set at the correct level. Report any concerns to the e-Safety Lead.
- Be aware of new and upcoming programmes, such as WhatsApp and Snapchat, that children are using and be aware of the age limit/risks associated with them. Regularly attend training for updates on changes to the curriculum and the requirements of teachers.
- 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 e-Safety incident.
- Communicate with current or past pupils, and their parents/carers, via school authorised channels only (i.e. using professional email addresses and telephone numbers). All communications with young people should be for school purposes only, unless otherwise authorised by the Headteacher, to minimise the risk of allegations being made against staff.
- Personal communications (such as social networking links) with young people currently in their care are strictly prohibited.
- Understand that behaviour in their personal lives may impact upon their work with children and young people if/when shared online or via social networking sites.
- Ensure that if a social networking site is used, details are not shared with children and young people and privacy settings are set to a maximum.
- Keep usernames and passwords private and never leave work stations unattended when logged in.
- Report accidental access to inappropriate materials to the e-Safety Leader to allow for sites to be added to the restricted list.

- Be mindful of transportation of sensitive pupil/colleague information and photographs on memory sticks, laptops or other devices between school and home. Wherever possible, encryption or password protection should be used to restrict unauthorised access in the event of loss or theft.
- Address e-safety incidents regularly throughout the year and ensure that sessions are planned into the curriculum to remind children to the importance of staying safe online. Plan in opportunities for children to put their knowledge of e-safety into practice.

4.4 Children and young people

Children and young people are responsible for:

- Signing agreement to, and abiding by, the Acceptable Use Rules set.
- Using the internet and technologies in a safe and responsible manner within school and at home.
- Informing staff of any inappropriate materials or contact from strangers immediately, without reprimand (age and activity dependent)
- Actively participating in the development and annual review of the Acceptable Use Rules.

5. Appropriate and Inappropriate Use

5.1 By staff of adults

To ensure that both young people and staff are appropriately safeguarded against online risks and allegations, a copy of the Acceptable Use Policy will be made accessible to all. The policy clearly highlights any behaviours or practices, linked to staff use of technologies, which are deemed inappropriate by HM Government 'Safer Working Practice' guidelines or other relevant safeguarding legislation and professional standards. Staff are expected to take responsibility for their own use of technology and are asked to read and sign acceptance of the staff acceptable use rules annually (see Appendix 1 for template).

Examples of inappropriate use:

- Accepting or requesting current or past pupils as 'friends' on social networking sites, or exchanging personal email addresses or mobile phone numbers.
- Behaving in a manner which would lead any reasonable person to question a staff member's suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on either the individual, their colleagues or the school/workplace.

In the event of inappropriate use

If a member of staff is believed to misuse the internet or learning platform in an illegal, inappropriate or abusive manner, a report must be made to the Headteacher/Safeguarding Lead immediately and the e-Safety Incident Flowchart referred to (see Appendix 2). The appropriate LSCBN allegation procedures and child protection policies must be followed to deal with any misconduct and all relevant authorities contacted.
In the lesser event of minor or accidental misuse, internal staff disciplinary procedures will be referred to in terms of any action to be taken.

5.2 By Children or Young People

The student Acceptable Use Rules provide children and young people with clear guidelines on appropriate use of the internet and technologies within school and are linked to school disciplinary procedures. Students sign acceptance of the rules when they join the school and they are displayed throughout the school as a reminder. To encourage parental/carer support of the student Acceptable Use Rules, a copy is sent home with the related school sanctions for misuse. This is also displayed on the school website and is clearly seen around school.
Parents/carers are asked to sign the Acceptable Use Rules with their child annually to show their support of the online safeguarding rules in place (see Appendix 3 for template).

In the event of inappropriate use

If a child or young person is found to misuse online technologies or equipment whilst at school, the following sanctions will apply:

- Failure to abide by Acceptable Use Rules and deliberate misuse of the internet/technologies will result in a letter being 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 withdrawal of a student's internet privileges for a period of time and another letter 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.

In the event of accidental access to inappropriate materials, students are expected to notify an adult immediately and attempt to minimise or close the content until an adult can take action.

In the event of a member of staff being aware of a child having a Facebook/twitter account, a letter will be sent home to their parents informing them of this and reminding them of the legal age requirement. Appropriate eSafety incident procedures are then followed.

6. The Curriculum

6.1 Internet use

It is the responsibility of schools to teach their students how to use the internet safely and responsibly. The following concepts, skills and competencies will be developed through both the PSHE and ICT curriculum:

- Internet literacy
- making good judgements about websites and emails received
- knowledge of risks such as viruses and opening mail from a stranger
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading personal information – what is and is not safe
- where to go for advice and how to report abuse.

It is also the school's responsibility to plan in opportunities for children to make informed judgements and manage risks themselves rather than relying on filtering systems.

Online personal safety is taken extremely seriously within school communities and students are encouraged to refrain from sharing personal information in any form of electronic communications. Personal informal includes:

- full name
- address
- telephone number
- email address

6.2 Pupils with additional learning needs

The school strives to provide access to a broad and balanced curriculum for all learners and recognises 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.

6.3 Email use

Students

The school has set up individual class email addresses for students to use as a class, as part of their entitlement to understand different ways of communicating and using ICT to share and present information. Students will use this email account for any form of school related communications (i.e. homework) and teaching staff will regularly monitor their class use of these systems. Teachers may want to pass this on to parents as a form of communication. Children's emails are set as their first name and second name followed by the school. If there are any cases where a child (for safeguarding purposes) cannot use this set up, alternative options should be offered, such as the email being turned off or directed to the class teacher. Children should be encouraged to update their password every three months to include a mixture of upper and lower case letters along with numbers. They should not use this email to sign up for any other sites.

Staff

Professional email addresses will be used for all electronic correspondence between staff and students, and for school related business only. This is true also for any communications with parents or carers. Under no circumstances will staff members engage in personal communications (i.e. via Hotmail or Yahoo accounts) with current or former students outside of authorised school systems. The use of professional email accounts allows for content monitoring to take place and minimises the risk of allegations being made against staff. Passwords should also be changed every three months for laptops and email accounts.

6.4 Mobile technologies

Everyday technologies, including mobile phones, mp3 players, tablets and handheld games consoles, are increasingly being used by both adults and children within the school environment. For this reason, appropriate safeguards must be in place to protect young people and staff against the following associated risks:

- Inappropriate or bullying text messages
- Images or video taken of adults or peers without permission
- Videoing violent, unpleasant or abusive acts towards a peer or adult which may be distributed
- Sexting - the sending of suggestive or sexually explicit personal images via mobile phones
- Wireless internet access which can bypass school filtering and allow access to inappropriate or potentially harmful material or communications.

All teachers have their own class mobile devices to use when taking photos. No personal devices or mobile phones should be used for this. Devices are regularly monitored and wiped clear throughout the academic year.

6.4.1 Mobile phones

Student Use:

Students are advised NOT to bring mobile phones to school. If there is no alternative, they are kept in the school office for safekeeping. If there is reason to suspect that a student's mobile device contains inappropriate, illegal or harmful content, whilst on school grounds, it will be confiscated by staff and may be searched. The e-Safety Incident flowchart and Child Protection procedures will be followed if such content is discovered.

Staff Use:

Staff may bring personal mobile phones into school, but they will be used outside of lesson time only. Under no circumstances will staff use their personal mobile phone to communicate with current or former students or their parents/carers. School telephone numbers or mobile phones will be used for this purpose, apart from when on off-site school trips. All images or video recordings of children and young people will be taken using school equipment, never personal camera phones or other such devices. It is the responsibility of staff to ensure that no inappropriate or illegal content is stored on their device when bringing it onto school grounds.

6.4.2 Laptops/Tablets

Teaching staff are provided with school laptops/tablets to allow for school related work to be completed off site. All school/Trust laptops and mobile devices must be password secured. Personal use of school issued computing facilities is permitted providing it is kept to a minimum and does not interfere with the employee's work. Sensitive data and school authorised images of students should not be stored on school laptops without appropriate encryption software in place. In the event that a laptop/tablet is stolen or lost there is potential for this content to be viewed by unauthorised individuals. Appropriate encryption also applies also to the use of any mobile memory devices.

6.5 Video and photographs

Images or videos featuring students will only feature on the school website or in press coverage if permission has been granted by parents/carers in advance. Wherever possible group shots of children will be taken, as opposed to images of an individual, and first names only will be displayed. Photographs should not show children in compromising positions or in inappropriate clothing (e.g. gym kit, swimming costumes).

School equipment will be used to take any images of students, and pictures should be removed from cameras and utilised appropriately within 24 hours of being taken. This is to ensure that images of students cannot be viewed by unauthorised individuals in the event of loss or theft.

6.6 Video-conferencing and webcams

To safeguard staff and young users, publicly accessible webcams are not to be used in school. As with video and photographs, permission will be sought from parents/carers before a child engages in video conferencing with individuals or groups outside of the school setting (e.g. communicating with a school overseas). All video conferencing will be supervised by staff and a record of dates, times and participants held in school for audit trail purposes.

7. Web 2.0 Technologies

7.1 Managing Social Networking and other Web 2.0 technologies

Social networking is now the communication form of choice for many adults and young people worldwide and, as a result, safeguards must be in place to ensure that staff and students are aware of the risks associated with this form of technology. To address this issue, a series of preventative measures are in place.

- Access to social networking sites is controlled through the school internet filtering systems. In KS2, Yammer may be used for classes to share information. This should remain a closed domain and no external people should be invited to the group. Children should avoid direct messaging (DM) teachers and instead post on the threads. Teachers are to regularly monitor use and plan in opportunities for children to explore the benefits of social media within a controlled and safe environment.
- Students and staff are discouraged from providing personal details or identifiable information on profiles (e.g. mobile number, address, school name, clubs attended, email address or full names of friends). Children are asked to include images of avatars for their display icon instead of real pictures.
- Students and staff are made aware of the risks of posting images online and how publicly accessible their content is. Background images in photographs which may reveal personal details should also be addressed (e.g. house number, street name, school uniform).
- Social networking security settings should be taught, and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking of unwanted communications is also highlighted.
- Comments on the blogs are regularly monitored, with the teacher modelling appropriate responses which should be left.
- Both online and school systems for reporting abuse or unpleasant content, i.e. cyberbullying, are reinforced www.thinkuknow.co.uk.

7.2 Staff using social networks

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, staff have a responsibility to ensure that their actions outside of school do not impact on their work with children and young people. HM Gov 'Safer Working Practice' clearly states that adults working with children should:

- Only make contact with students for professional reasons and with the authorisation of the Headteacher. Any communication should be via professional email only and never through a personal email account.
- Ensure that if a social networking account is used, details are not shared with children and young people and privacy settings are set to a maximum.
- Be aware that behaviour in their personal lives may impact on their work with children and young people.
- Not behave in a manner which would lead any reasonable person to question their suitability to work with children and young people.

8. Safeguarding measures

Under the Counter-Terrorism and Security Act 2015, which came into force on 1 July 2015, there is a requirement that schools "have due regard to the need to prevent pupils being drawn into terrorism." The school uses Policy Central Enterprise which is installed onto all child devices in the school. This software detects key words which are either typed in or appear on the screen. An image is taken of the screen and logged in the central system. The device, year group, time and content are then listed. Weekly monitoring takes place, with each 'hit' being reviewed and categorised. Any further action required is done so by the e-safety lead. Repeated incidents are logs to form a history if needed.

8.1 Filtering

The *Exa Networks* filtering system provides a filtered internet service to NPAT Schools, enabling them to assign appropriate levels of access to pupils and staff depending on role, age and maturity. To safeguard young users from viewing inappropriate content, all filtering must be set to 'No Access' and then individual access controlled via:

- Level 3: EMBC standard younger pupil's policy

The school also has:

- Local Control – the school controls access to websites and has the option to add to a 'restricted list'.

In addition to the above, the following safeguards are also in place:

- Annually, the Headteacher will sign a disclaimer stating agreement to the filtering levels being maintained as part of the connectivity to broadband by *Exa Networks*. In the event that the default site level is not set to 'No Access', the Headteacher and Governors will be asked to write a letter NPAT explaining how they intend to safeguard their children and young people (e.g. using an appropriate accredited service such as *Netsweeper* or School Guardian so that the minimum of *Becta* Level 4 is met).
- Anti-virus and anti-spyware software are 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.
- Links to e-safety websites are provided on the school website.
- Encryption codes on wireless systems prevent hacking.

8.2 Tools for bypassing filtering

Web proxies are the most popular and successful method for students to bypass internet filters in order to access unauthorised online content on the school network. A web proxy is capable of hiding the IP address of the user and opening unrestricted and, in cases, unidentifiable channels through which blocked material can be viewed e.g.

Social networking sites, gaming websites or adult content. To manage this safeguarding concern, students and staff are forbidden to use any technology designed to circumvent, avoid or bypass school security controls (including internet filters, antivirus solutions or firewalls). Violation of this rule by either staff or students will result in school sanctions being applied.

9. Parents

9.1 Roles

Each student will receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school. Students and their parents/carers are asked to read and sign acceptance of the student Acceptable Use Rules to be returned to, and stored by, the school. Parents are also encouraged to attend annual E-safety workshops to highlight the issues surrounding young people today and technology.

9.2 Support

As part of the school's approach to developing e-safety awareness with children and young people, every effort is made to offer parents/carers the opportunity to find out more about how they can support their child to stay safe online within and beyond the school environment. E-safety Parent/Carer Information Sessions will be held annually to raise awareness of key internet safety issues and highlight safeguards currently in place at school (e.g. filtering and training in place to minimise online risk.) Free to order resources from *Childnet* (http://www.childnet-int.org/kia/parents/) and the *Thinkuknow* website (http://www.thinkuknow.co.uk/teachers/resources/) can be used to support this. Wherever possible, the school will endeavour to provide internet access for parents/carers without this resource at home to ensure that appropriate advice and information on this topic can be viewed.

10. Links to other policies

10.1 Behaviour, Cyberbullying and Anti-Bullying

The Acceptable Use Policy is cross-referenced throughout a number of other policies in place throughout the school, including those for behaviour, anti-bullying, PSHE and child protection.
Cyberbullying features within the school's anti-bullying policy due to the growing number of incidents recorded. Cyberbullying will not be tolerated in or outside of school and clear procedures for dealing with cyberbullying incidents can be found within the anti-bullying policy.

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

The LSCBN Allegations Procedure www.proceduresonline.com/northamptonshire/scb/ will be referred to in the event that an allegation of misuse or misconduct is made by a child or other adult about a member of staff. Allegations made against staff members must be reported to the Designated Person for Child Protection within school immediately. In the event of an allegation being made against the Headteacher, the Chair of Governors will be notified immediately.

10.3 PSHE

The teaching and learning of e-Safety is 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 offline.

10.4 School website

Permission will be sought from parents/carers prior to the uploading of any images onto the school website. Consideration is given to which information is relevant to share with the general public on a website and secure areas will be used for information pertaining to specific audiences. The schools AUP will also be published on this platform along with recommended websites.

10.5 Disciplinary Procedure for All School Based Staff

In the event that a staff member is seen to be in breach of professional standards of conduct or is believed to have misused online technologies, school disciplinary procedures and sanctions will be applied.

Appendix 1 - Staff Acceptable Use of Technologies Agreement

To ensure that all staff are confident in their use of technologies and the internet, the Acceptable Use Rules have been developed in collaboration with education professionals and unions. The core values of the Acceptable Use Policy are safeguarding and responsible behaviours allowing young people, and the adults who surround them, to safely enjoy all of the benefits that technology can offer. To assist with this, the full Acceptable Use Policy is accessible to all staff members and should be referred to for further information.

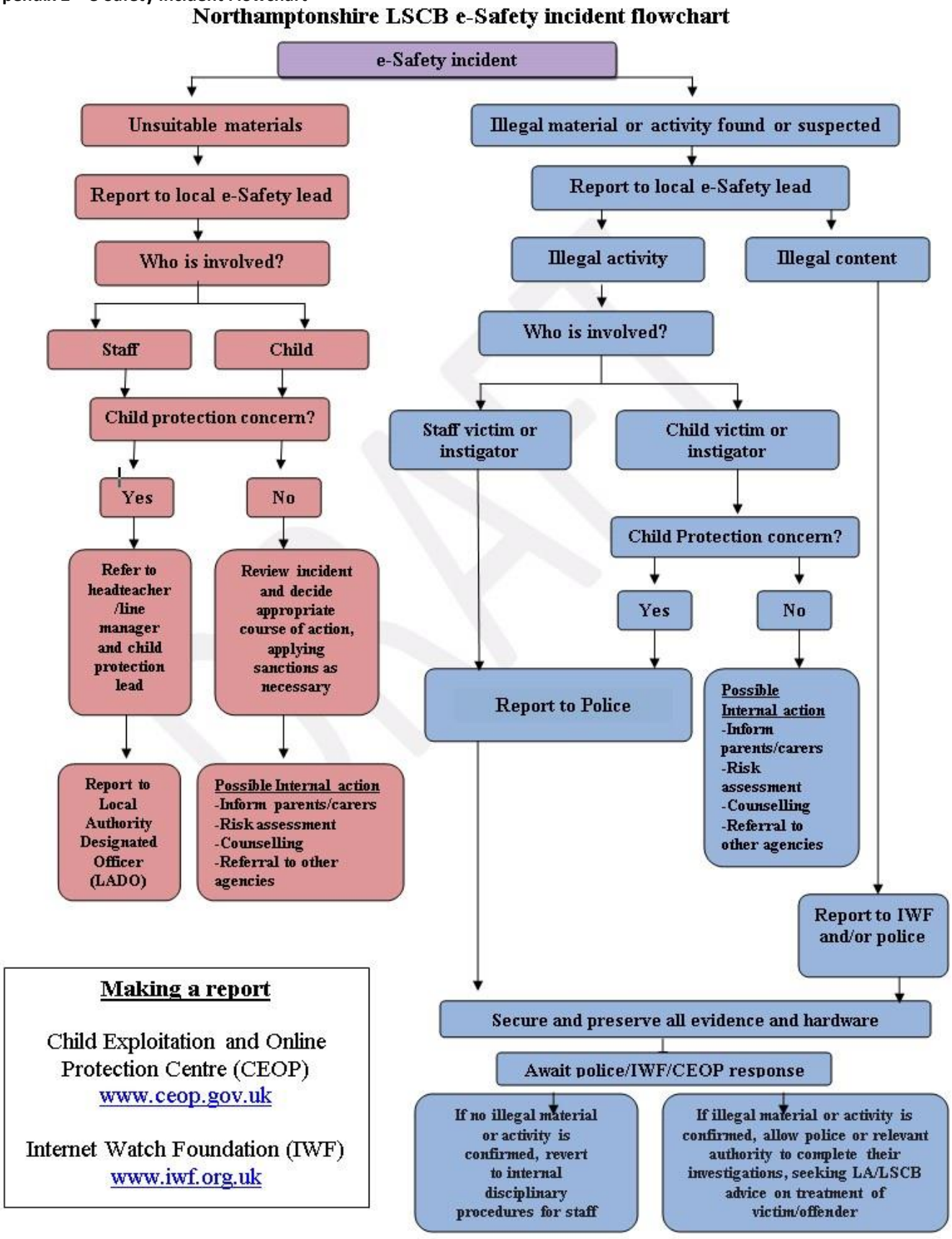
e-Safety Lead:
Designated Persons for Child Protection are: Mr Darren Smith
Mrs Karen Smith
Mrs Sharon Ritchie

- I know that I should only use the school equipment in an appropriate manner and for professional use, unless otherwise agreed by the Headteacher.
- I understand that I must not have personal communications with current, or former pupils, outside of my professional role. This includes establishing social networking 'friendships' on sites such as Facebook, or sharing personal phone numbers or email addresses. Any school related communication should be conducted through professional email accounts or telephone numbers only.
- I understand that I should not behave in a manner, either within or outside of the work environment, which would lead any reasonable person to question my suitability to work with children or act as a role model. This would include inappropriate comments, photographs or videos on social networking sites which reflect badly on myself, my colleagues or the school.
- I know that permission must be received from parents/carers before images of children are used online (e.g. school website). I understand that images must be appropriate and should not reveal any personal information.
- I know that any photographs taken of children for work purposes should be done so using school equipment only. Personal cameras should not be used.
- I understand that any incidents of concern for children's safety must be reported to the Headteacher, Designated Person for Child Protection or e-Safety Lead in accordance with procedures listed in the Acceptable Use Policy.
- I know where to access a copy of the e-Safety Incident Flowchart should an incident of misuse arise.
- I understand that the school email system and school issued devices are routinely monitored as part of our commitment to safeguard young users.
- I know that each user should be accessing the internet with their unique username and password for filtering and safeguarding purposes. For this reason, I will keep my password private and for my own use only.
- I will raise any concerns regarding school ICT use with my line manager to avoid possible misunderstandings.
- I have access to a copy of the full Acceptable Use Policy should I need to refer to the document about any e-Safety issues or procedures.

I have read, understood and agree to the above Acceptable Use Rules. I understand that these rules are in place to ensure that staff are aware of their professional responsibilities to safeguard children when accessing online technologies.

Signed: …….. Dated: ……

Appendix 2 – e-Safety Incident Flowchart



There are three instances when you must report directly to the police.

- Indecent images of children found (i.e. under 18 years of a sexual nature)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

If an indecent image is found CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions. The police 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 turn off the machine. The Internet Watch Foundation www.iwf.org.uk offers further support and advice in dealing with offensive images online. It is important to remember that any offensive images received should never be forwarded, 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.

Appendix 3 - Parent/Carer and Child Acceptable Use Agreement

Dear Parents/Carers,

As part of an enriched curriculum, your child will be accessing the internet, school email and virtual learning environment via a filtered service provided by the *EXA Network*. In order to support the school in educating students about safe use of the internet, we are asking parents and children to read and sign acceptance of the attached acceptable use rules. Completed forms should be returned to the school as soon as possible.

The rules provide an opportunity for further discussions with your child about safe and appropriate use of the internet and other online tools (e.g. mobile phones), both within and beyond school (e.g. at a friend's house or at home). Sanctions in place for misuse of technologies and subsequent breach of the rules are detailed in the full Acceptable Use of Technologies Policy which parents/carers are welcome to view.

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

Yours faithfully,

Headteacher

Acceptable Use Rules Return Slip

Child Agreement:

Name: _____Class:_____

- I understand the rules for using the internet and email 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, email and other online tools.
- I understand that filtering can never be completely fool proof and occasionally inappropriate materials may be accessed. I accept that the school will endeavour to deal with any incident that may arise swiftly and according to policy.
- I understand that my child's safe use of the internet and online technologies outside of school is my responsibility.

Parent/Carer Signature: _____ Date: _____

Key Stage 1 Online Rules

These are our rules for using the internet safely.

Our Online Rules

- We learn how to use the internet safely.
- We can send and open messages with an adult.
- We can write polite and friendly emails 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 the internet safely.
- We can go to www.thinkuknow.co.uk for help.

Key Stage 2 Online Rules

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

Our Online Rules

- We use the internet to help us learn and we know how to use it safely and responsibly.
- We send emails and messages that are polite and friendly.
- We will only email, chat or go on webcam with people that we know in real life, with permission from our teachers or parents.
- We make sure that an adult always knows when we are online.
- We never give out passwords or personal information (like our full name, school or address).
- We never post photographs without permission and never include names with photographs.
- We know who to ask if we need help.
- If we see anything on the internet or on email that is scary or makes us feel uncomfortable, we know what to do.
- We never open emails or links from people we don't know.
- We know that the rules are there to keep us safe and must not be broken.
- We are able to keep ourselves and each other safe by using the internet in a responsible way.
- We can go to www.thinuknow.co.uk for help

Further Information and Guidance

- 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 information and resources for children, teenagers, parents/carers and professionals
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk (all under 11)
- www.phonebrain.org.uk (for Years 5 – 8)
- www.bbc.co.uk/cbbc/help/web/staysafe (for Years 3/4)
- www.hectorsworld.com (for FS, Year 1 and 2 and is part of the *thinkuknow* website above)
- www.education.gov.uk (for adults and professionals

- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)

Signed _____

Dated_____

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. ICT lead will add this site to the banned list immediately.

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.

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.
- ICT lead will add site to the banned list immediately.

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.

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.