Bozeat Community Primary School & Nursery

Acceptable Use and Online Safety Policy

Approved by:	Full Governing Body
Last reviewed on:	March 2023
Next review due by:	March 2024

The Online-Safety Lead for Bozeat Primary School is: Gareth Rust
The Designated Persons for Child Protection are: Gareth Rust and Michele Parker

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 ever changing nature of emerging technologies within the curriculum and media and highlights the need for regular review to incorporate development within ICT (Information Communication Technology) . 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
- Facetime, WhatsApp and other video calling such as Zoom.
- 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
- Awareness of such safeguarding issues, such as upskirting and peer-on-peer abuse
- Social and emotional effects of an increased use of technology
- Financial impact, such as gambling or gaming which may involve monetary purchases

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 Head of School and Governors

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

- The Head of School has designated an Online-Safety Lead to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring Online-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 Online-Safety Lead and staff to be trained and update policies, where appropriate.

- The Head of School promotes Online-Safety across the curriculum and has an awareness of how this is being developed and linked with the school development plan.

- The Head of School will inform the Governors at all meetings about the progress of or any updates to the OnlineSafety curriculum (via PSHE or ICT) and ensure they know how this relates to child protection.

- The Governors must ensure that Online-Safety is embedded within all Child Protection training, guidance and practices.

- An Online-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 Online-Safety incidents

4.2 Online-Safety Lead

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

- Recognise the importance of online-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 all adults understand how filtering levels operate and their purpose.
- Report issues and update the Head of School 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 and via alerts from SENSO monitoring systems.
- Maintain an Online-Safety Incident Log, which is attached to the policy, is to be shared with the Head of School and Governors at agreed intervals.
- Monitor how Online-Safety is taught throughout EYFS, 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, 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 Online-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 Online-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 Head of School, 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 Online-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 online-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 online-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 or other adults

To ensure that both young people and staff are appropriately safeguarded against online risks and allegations, a copy of the NVP Acceptable Use Policy will be made accessible to all and signed by all staff working in school.

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 NVP acceptable use policy for more information.

In the event of inappropriate use

If a member of staff is believed to have misused the internet or learning platform in an illegal, inappropriate or abusive manner, a report must be made to the Head of School/Safeguarding Lead immediately and the Online-Safety Incident Flowchart referred to (see Appendix 2). The appropriate LSCBN (Local Safeguarding Children's Board Northamptonshire) 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. 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 1 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.

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.
- awareness of fake news.

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 online-safety awareness sessions and internet access.

6.3 Email use

Staff

Class teams accounts will be used for all electronic correspondence between staff and students, and for school related business only. Communications with parents or carers will be via professional email addresses only. Under no circumstances will staff members engage in personal communications (i.e. via Hotmail or Yahoo accounts) with current or former students or parents. The use of professional email accounts allows for content monitoring to take place and minimises the risk of allegations being made against staff.

6.4 Mobile technologies

Everyday technologies, including mobile phones, smartwatches, 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.
- Upskirting and peer-on-peer abuse.

Only School devices should be used 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.

Mobile phones

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 Online 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.

6.5 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. 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 SENSO software 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 online-safety lead. Repeated incidents are logs to form a history if needed.

8. Filtering

The filtering system provides a filtered internet service to school, enabling them to assign appropriate levels of access to pupils and staff depending on role, age and maturity. Wollaston IT department manage the filter setting and any changes to content is done with in discussion with the Head of School.

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 which is returned to, and stored by, the school.

Parents are also encouraged to attend regular online-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.

Online-safety Parent/Carer Information Sessions will be held on a regular basis 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.

The school will also use the services of Northamptonshire's Online Safety and Wellbeing Officer.

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.

Appendix 1 - 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. 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 Head of School.

Yours faithfully,
Head of School

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: _____

Acceptable Use agreement for (KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child):

EYFS, Reception and Year 1 to sign as a class during an online safety lesson

Acceptable Use agreement for Key Stage 2

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I will ask permission from a teacher before using any technology devices.
- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone will steal it.
- I will be aware of "stranger danger", when I am communicating online.
- I will not share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material, messages, or anything that makes me feel uncomfortable when I see it on-line.
- I will not access other people's files or send pictures of anyone without their permission.
- I understand that the school systems and devices are for educational use and that I will not use them for personal or recreational use unless I have permission.
- When I am using the internet to find information, I will check that the information is accurate.
- I will not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube).
- I will be polite and responsible when I communicate with others, I will not use inappropriate language and I understand that it is ok for others to have different opinions from me.
- I understand that if I do not follow the Acceptable Use Agreement I may not be allowed to use any technology devices in school and my parents/carers may be contacted.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school.

Your name: Class: Date:

Key Stage One Online Rules

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

- 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

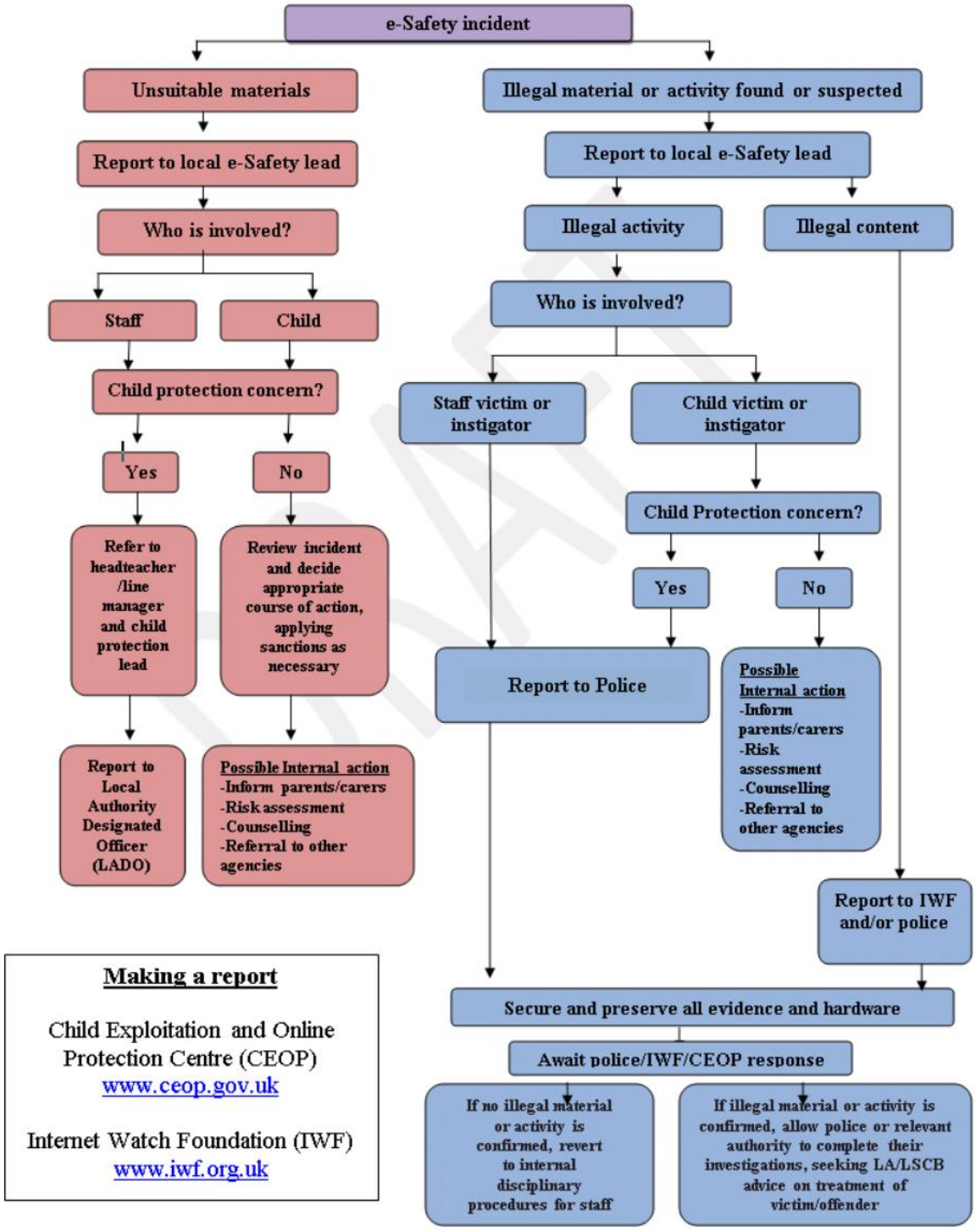
These are our rules for using the internet safely and responsibly.

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

Appendix 2 – e-Safety Incident Flowchart

Northamptonshire LSCB e-Safety incident flowchart



Making a report

Child Exploitation and Online Protection Centre (CEOP)
www.ceop.gov.uk

Internet Watch Foundation (IWF)
www.iwf.org.uk

Further Information and Guidance

- 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.education.gov.uk (for adults and professionals
- www.digizen.org.uk(for materials around the issue of cyberbullying)
- https://saferinternet.org.uk/ (for helpful advice about accessing the internet)
- www.internetmatters.org (for advice for parents/carers and schools)
- https://nationalonlinesafety.com/guides (free helpful guides which are updated weekly about all aspects of online safety).