# Kislingbury CEVC Primary School

# E- Safety Policy

| | |
|---|---|
| Policy Review Committee | Pupils and Personnel Committee |
| Policy Last Reviewed | October 2017 |
| Policy Review Schedule | Annual |
| Policy Review Date | Autumn 2018 |

# Introduction

Materials on the Northamptonshire County Council Website have been used to inform this policy. It is adapted to suit our primary setting from the Northamptonshire local Safeguarding Children Board E-Safety Policy.
http://www.northamptonshire.gov.uk/en/councilservices/EducationandLearning/services/e-safety

This policy has been developed to ensure that all adults in Kislingbury CE Primary School are working together to safeguard and promote the welfare of children and young people. Please also refer to the L.A. Acceptable Use Policy.

# Policy Statement

IT and the internet have become integral to teaching and learning within our school; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button. At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Social Media, including Facebook and Twitter
- Web enabled mobile/smart phones
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Video broadcasting, including Chat Roulette, Omegle
- Blogs and Wikis
- Email, Instant Messaging and Chat Rooms

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial.

All schools have a duty 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 that children, young people and staff continue to be protected.

## 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 of, the school environment.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

## Scope of Policy

This policy applies to all staff, pupils, governors, visitors and contractors accessing the internet or using technological devices on school premises. This includes staff or pupil use of personal devices, such as mobile phones or ipads which are brought onto school grounds. This policy is also applicable where staff or individuals have been provided with school issued devices for use off-site, such as school laptop or work mobile phone.

# Staff Responsibilities

### Teaching and Support Staff (including volunteers)

All staff have a shared responsibility to ensure that children and young people are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all who work in schools are bound.

Please see The Local Authority Acceptable Use Policy for School Based Employees for further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email or related technologies within and beyond school. A copy of this document is made available to all staff and shared with any volunteers, visitors or contractors.

## Network Manager/Technical Staff

The School uses an outside contractor for technical services, and it is the responsibility of the school to ensure that the managed service provider carries out all of the safety measures that would be expected of the school's technical staff, including being provided with the School e- Safety Policy and Staff A.U.P.

The ICT Technician/ ICT Co-ordinator is responsible for ensuring:

- that the school's ICT infrastructure is secure and not open to misuse or malicious attack.
- that anti-virus software is installed and maintained on all school machines and portable devices.
- that the school's filtering system is applied and updated on a regular basis and that responsibility for its implementation is shared with the E Safety Lead and the Designated Person for Safeguarding.
- that any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the e Safety Incident Log.
- that users may only access the school's network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- that he/she keeps up to date with e safety technical information in order to maintain the security of the school network and safeguard children and young people.
- that the use of the school network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead.
- that the system logs any miss use and that the HT / E-Safety lead is notified of incidents of miss use.
- A log of any incidents will be reported to the Pand P Committee termly. Please see Appendix 1

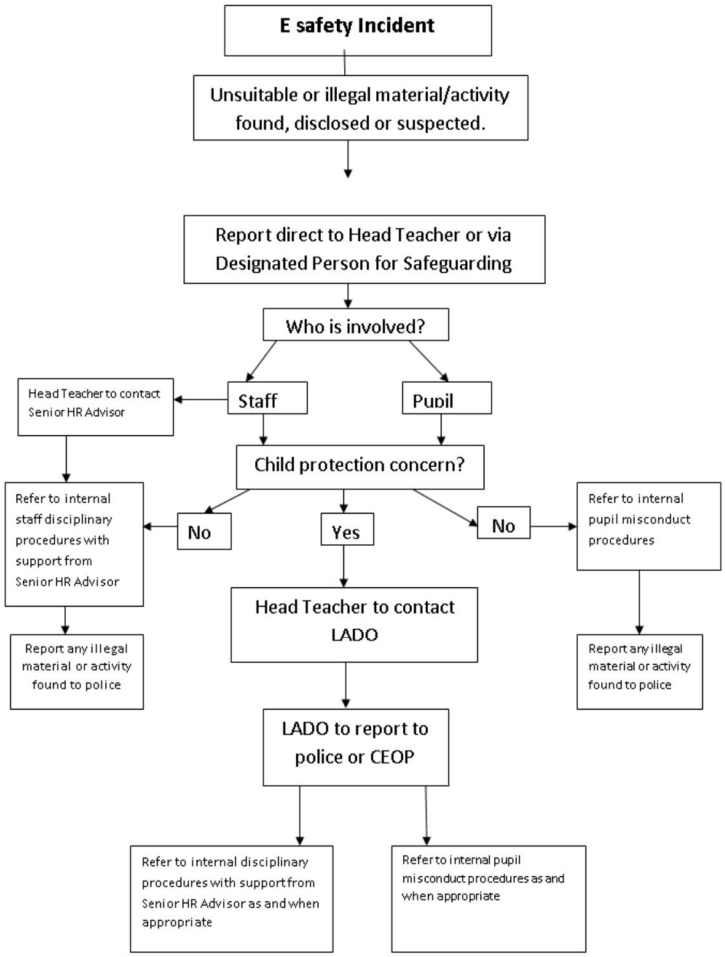
## Children and Young People

Children and young people are responsible for:

- Using the internet and technologies in a safe and responsible manner within school.
- Informing staff of any inappropriate materials, cyberbullying or contact from unknown sources.

# Incident Reporting

In the event of misuse by staff or students, including use of the school network in an illegal, unsuitable or abusive manner, a report must be made to the Head teacher/Designated Person for Safeguarding immediately and the e-Safety Incident Flowchart followed.




In the event of minor or accidental misuse, internal investigations should be initiated and disciplinary procedures followed where appropriate. Additionally, all security breaches, lost/stolen equipment or data, unauthorised use or suspected misuse of ICT should be reported immediately to the Head Teacher and Network IT technician.

All incidents must be recorded on the E Safety Incident Log to allow for monitoring, auditing and identification of specific concerns or trends.

## Monitoring

School IT Lead staff  monitor and record user activity, including any personal use of the school IT system (both within and outside of the school environment) and users are made aware of this in the Acceptable Use Policy.

## The Curriculum

The school strives to embed e Safety in all areas of our curriculum and key online safeguarding messages are reinforced wherever IT is used in learning.

- The school follows the NCC guidance and the Rising Stars Computing  Scheme of Work which incorporates annual online safeguarding units from for all year groups with National Curriculum statutory objectives for Computing.
- Pupils are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the internet as part of the e Safety curriculum.
- Opportunities for informal discussions with students about online risks and strategies for protecting yourself online are built into our curriculum, to ensure that our students are armed with accurate information.
- Students, parents and staff are signposted to national and local organisations for further support and advice relating to e safety issues, including Beat Bullying, Childline and CEOP

## Pupils with special Educational 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.

## E-Mail Use

### Staff

- The school provides all staff with an email account on the learning platform which must be used for all communication with pupils. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

- Under no circumstances will staff members engage in any personal communications (i.e. via hotmail or yahoo accounts) with current or former students outside of authorised school systems.
- All emails should be professional in tone and checked carefully before sending, just as an official school letter would be.
- Staff should inform their line manager or the e Safety Lead if they receive an offensive or inappropriate email via the school system.

### Students

- The school provides individual email accounts on the Learning Platform for students to use as part of their entitlement to understand different ways of communicating and using ICT to share and present information.
- Students will use their school issued email account for any school related communications, including where appropriate homework or correspondence with teachers. Email content will be subject to monitoring and filtering for safeguarding purposes.
- Students will be taught about email safety issues, such as the risk of exposing personal information, opening attachments from unknown sources and the management of inappropriate emails. Students will also be guided in the correct tone to use in email correspondence and regularly reminded of restrictions on abusive or inappropriate content.
- The forwarding of chain letters is strictly prohibited in school and should be reported to a member of staff immediately.

### Both

- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the e Safety Lead. Account holders must never share their password with another user, or allow access to their email account without the express permission of the Head Teacher.

## Managing Remote Access

As technology continues to develop at an exponential rate, schools and their staff are increasingly taking advantage of opportunities for off-site access to the school Learning Platform and email using remote access facilities. For data security and safeguarding purposes, it is crucial that staff are aware of the following restrictions on use:

- Only equipment with the appropriate level of security should be used for remote access
- Any documents that hold sensitive information must be written at school and only saved to the network.
- Log-on IDs and PINs should be confidential and use information that cannot be easily guessed (e.g. date of birth, telephone number, number patterns)
- For security purposes, network access information should not be written down or stored with the device in case of theft or unauthorised access.

## Internet Access and Age Appropriate Filtering

### Broadband Provider: Exa Networks

All students are entitled to safe and secure internet access and schools have a duty to deliver this as part of the learning experience. The Head teacher is ultimately responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that age appropriate internet filtering is in place to protect young users from inappropriate or harmful online content. To this end, the school has the following filtering measures in place:

- Filtering levels are managed and monitored on behalf of the school by our broadband supplier and technical support, allowing an authorised school staff member to allow or block access to site and manage user internet access.

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

- Anti-virus and anti-spyware software is used on all network and stand alone PCs of laptops and is updated on a regular basis.
- A firewall ensures that information about children and young people cannot be accessed by unauthorised users.
- Encryption codes on wireless systems prevent hacking.

Students

- Primary age appropriate search engines are used in school as an additional safeguard.
- CEOP's Hector Protector is in use on all devices accessed by students to provide a shield for young people should they access inappropriate content at any point.
- Every child's log in page includes a CEOP button.

## Staff

- Expectations for staff online conduct is addressed in the NCC Acceptable Use Policy for School based employees.
- Staff are required to preview any websites before use, including those which are recommended to students and parents for homework support.

## Use of School and Personal IT equipment

### School ICT Equipment

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the School Bursar and ICT Co-ordinator.
- Personal or sensitive data is not stored on school devices (e.g. laptops, ipads, PC or USB Memory Sticks). This is true also of any photographs or videos of students, such as class photos or assembly evidence. All such material should be stored either on the school network or on an encrypted device.
- Time locking screensavers are in place on all devices in school to prevent unauthorised access, particularly on devices which store personal or sensitive data.
- Personal ICT equipment, such as laptops or memory sticks, must not be connected to the school network without explicit consent from the technician or ICT Co-ordinator and a thorough virus check.

### Mobile/Smart Phones

### Student use:

- Students are not permitted to bring mobile phones/devices onto school grounds unless express permission has been granted by the Head Teacher for exceptional circumstances (e.g. independent journey to and from school)
- Where mobile phones have been allowed in the above circumstances, the device will be turned off and locked away by a responsible adult at the start of the school day and returned to the student before their homeward journey.

## Staff use:

- Personal mobile phones are permitted on school grounds, but should be used outside of lesson time only.
- It is the responsibility of the staff member to ensure that there is no illegal or inappropriate content stored on their device when brought onto school grounds.
- Personal mobile phones should never be used to contact children, young people or their families, nor should they be used to take videos or photographs of students. School issued devices **only** should be used in these situations.

## Laptops/ iPads

- Staff must ensure that all sensitive school data is stored on the network (shared drive) and not on the laptop or device, unless the device is encrypted. In the event of loss or theft, failure to safeguard sensitive data could result in a serious security breach and subsequent fine. Password protection alone is not sufficient.
- Personal use of school laptops or computing facilities, whilst on site, is left to the discretion of the Head Teacher and may be permissible if kept to a minimum, used outside of lesson times and does not interfere with an employee's work.
- Staff are provided with laptops to allow for school related work to be completed off site. Personal use of the laptop from home (such as web browsing/online shopping etc) is permitted but should be kept to a minimum and use of the device is strictly restricted to the authorised member of staff only (i.e. not family members)
- Staff are aware that all activities carried out on school devices and systems, both within and outside of the school environment, will be monitored in accordance with this policy.
- Staff will ensure that school laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.

## Removable Media (Memory Sticks/USB)

- Where staff may require removable media to store or access sensitive data (e.g. IEPs, pupil attainment and assessment data) off site, only encrypted memory sticks will be used.
- Any passwords used for encrypted memory sticks/or other devices will be remain confidential to the user and shared only with authorised IT personnel for security and monitoring purposes.

## Photographs and Video

Digital photographs and videos are an important part of the learning experience for children and young people and, as such, schools have a responsibility to ensure that they not only educate students about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and young people about the use of digital imagery within school.

- Written consent will be obtained from parents or carers before photographs or videos of young people will be taken or used within the school environment, including the school website or associated marketing material. This will be on the child joining the school.
- Permission will be sought from any student or staff member before an image or video is taken and the purpose of the activity and intended use of the image will be made clear.
- Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Head Teacher for use of personal equipment for school related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device.
- Where photographs of students are published or displayed (e.g. on the school website) no names will be displayed only non-identifying captions (e.g. Year 4 pupil playing football)
- Wherever possible, group shots of students will be taken, as opposed to images of individuals and images should never show young people in compromising situations or inappropriate clothing (e.g. gym kit, swimming costumes)

## Parent / Carer Involvement

As part of the school's commitment to developing e-safety awareness amongst children and young people, every effort is made to engage parents and carers in the process.

- All students and their parents/carers will receive a copy of the Home School Agreement each year. Students and their parents/carers are both asked to read and sign acceptance of the rules, a copy of which will be stored at school.
- E Safety parent/carer sessions will be run annually to raise awareness of key internet safety issues and highlight safeguarding measures in school.
- Wherever possible, and subject to prior arrangement, the school will endeavour to provide parents/carers without internet access to research online safety materials and resources.
- E-Safety guidance and links to CEOP and On line safety advice for parents will be provided on the School Web site.

# Review

This policy will be reviewed annually or sooner if necessary, by the P and P committee. The last review was October 2016.

# Appendix 1

## Kislingbury School  E Safety Incident Log

Details of ALL eSafety incidents to be recorded by the eSafety Lead.  This incident log will be monitored termly by the Head teacher, Designated Person for Child protection and Safeguarding Governor.

| Date of incident | Name of individual(s) involved | Device number/location | Details of incident | Actions and reasons | Confirmed by |
|---|---|---|---|---|---|
| 1/10/10 | Joe Bloggs | PC 63 Rm 4 | Child accessed inappropriate chat site using child log-in. Adult language and pornographic images viewed. | Hector Protector launched effectively by young person. Synetrix help desk contacted. Website now blocked and filtering levels reviewed and altered. | Davey Jones (Deputy Head CPO) |
| | | | | | |
| | | | | | |
| | | | | | |