Northamptonshire Local Safeguarding Children Board

E Safety Policy

Waynflete Infants' School

Policy Statement

ICT and the internet have become integral to teaching and learning within schools; 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 or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

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 Waynflete Infants' School 'Internet Access and Acceptable Use Policy' 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 has an arrangement With Blue Planet Ltd to provide IT support and technical advice. The agreement is on a one month notice period and commenced on 1st June 2015.

The Network Manager/Systems Manager/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 policy 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.

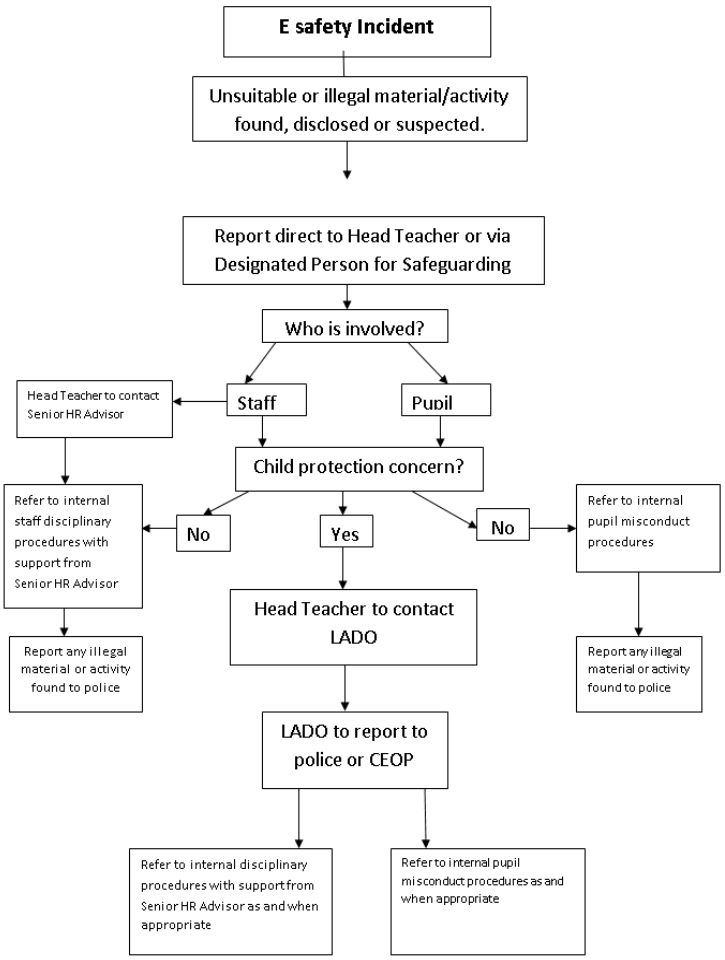
Children and Young People

Children and young people are responsible for:

- Signing agreement to, and abiding by, the Acceptable Use Rules for students; parents are asked to sign on their child's entry to the school.
- 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, Network Manager and Senior Information Risk Owner (SIRO)

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 ICT technical staff regularly monitor and record user activity, including any personal use of the school ICT 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 ICT is used in learning.

At Waynflete Infants' School, our ICT curriculum is in the form of our ICT Learning Journey, which includes a range of progressive skills from Reception to Year 2. The skills in Years 1 and 2 are based on **our scheme of work for ICT, Rising Stars Computing.**

In Year 1, the units are;

- **E-safety**
- **We are treasure hunters – using programmable toys**
- **We are TV chefs – Filming the steps of a recipe**
- **We are painters – Illustrating an e-book**
- **We are collectors – finding images using the web**
- **We are storytellers – producing a talking book**
- **We are celebrating – creating a card digitally**

In Year 2, the units are;

- **E-safety**
- **We are astronauts – programming on screen**
- **We are photographers – taking better pictures**
- **We are researchers – researching a topic**
- **We are detectives – collecting clues (email)**
- **We are zoologists – collecting data about bugs**
- **We are writers – using a word processor**

In Reception, they follow the Early Learning Goal for technology along with some specific skills, using the following headings:

- **Key skills**
- **Computing**
- **Reviewing, modifying and evaluating work**
- **E-safety**
-

Children are given a range of different opportunities to develop skills in these areas, with a cross-curricular approach being used by all Year groups.

For further information regarding the ICT curriculum at Waynflete Infants' School, please see our ICT Learning Journey.

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.

Email Use

Staff

- The school provides all staff with a professional email account to use for all school related business, including outside agencies, staff in other schools, Teaching students and university Tutors.
- Communication with parents should be in person, or e-mails can be sent to Headteacher, School Business Manager or the School Office Staff.
- 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.
- E-mails to parents should be via the Headteacher's or School Business manager's email account to ensure that all emails are monitored closely. Face to face contact or over the phone is the preferred method of communication.

Students

- At Waynflete Infants' School the children will have access to E-mail as a whole class only. They will use the class teachers' school E-mail account to send and receive E-mails to/from other members of staff / classes within the school.

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 network 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 using for remote access (i.e. encryption on any devices where sensitive data is stored or accessed)
- 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: **British Telecom**

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 in school via an administration tool/control panel, provided by our broadband supplier, which allows an

authorised staff member to instantly allow or block access to a site or specific pages and manage user internet access.

- Filtering levels are managed and monitored on behalf of the school by our broadband supplier or technical support, allowing an authorised school staff member to allow or block access to site and manage user internet access.
- Age appropriate content filtering is in place across the school, ensuring that staff and pupils receive different levels of filtered internet access in line with user requirements
- Staff have unique usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering.
- Class log-ins are used across the school for children to log on to the computers with suitable filtering levels in place.
- If teachers find they cannot access programmes or websites they have deemed suitable for children to use, they will request for the website to be unblocked.

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

The CEOP Report Abuse button is available on the school network to allow students or staff to report online safeguarding issues.

Primary

- Age appropriate search engines (e.g. Yahooligans or primaryschoolict.com) used in school as an additional safeguard.
- As part of ICT lessons, children will be taught what to do if they find something they do like or don't think they should be seeing; it is expected that children will first use the minimise button to remove the image / information from the screen, and then immediately let the teacher know what has happened.
- Children will have no unsupervised access to the Internet or computers, therefore there will always be an adult present for them to report to.

Staff

- Expectations for staff online conduct is addressed in the 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 ICT Equipment

School ICT Equipment

- Personal or sensitive data is not stored on school devices (e.g. laptops, ipads, PC or USB Memory Sticks) unless encryption software is in place. 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 Network Manager 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 under any circumstances.

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.
- It is expected that staff will have their mobile phones on silent in their bags away from the children and will not carry them on their person. In certain circumstances staff may carry their phone on their person, however the Headteacher should be informed of this.
- 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 solely 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.
- Staff are provided with laptops to allow for school related work to be completed off site. Staff will be able to use their work or home laptop to access all files and programs at school via RDS (Remote Desktop Services). This will be available via a website that can be accessed from home.
- 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)

- Staff will be able to access work from and save their work to the School Staff Shared Area from their home devices as long as they have an Internet Connection.

- No memory sticks are used in school.

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.
- At Waynflete Infants', permission for photographs to be used within school is sought on the child's entry to 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.

Video conferencing

- Permission is obtained from parents and carers prior to their child's involvement in video conferencing.
- All pupils are supervised by a member of staff when video conferencing, particularly when communicating with individuals or groups outside of the school environment (e.g. international schools)
- All video conferencing activities are time logged and dated with a list of participants.
- PLEASE NOTE – video conferencing is not currently used at Waynflete Infants' School, however should we have an opportunity to experience this in the future, we will be following the above guidelines.

Parent/Carer Involvement

As part of the schools 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 Acceptable Use Rules on first time entry to the school. 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 are being introduced with other cluster schools, including Magdalen College School, to raise awareness of key internet safety issues and highlight safeguarding measures in place within school.

- A joint e-safety meeting between WIS and Brackley Junior School was held for the first time in March 2016 and was attended by parents from both schools.

Waynflete Infant School Procedures .

Pupil access to the internet.

On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. Use of the internet will always be an adult-led activity; children will use the internet in the ICT suite with an adult present at all times. At no time will pupils be allowed unsupervised access and suitable filtering levels will be used on all computers where children are accessing the internet.

Children will use the internet for the following purposes:

- access to specific websites to search for information and specific photographs/images.
- access to specific websites to play educational games linked to their curriculum work.
- use of search engines to find specific images to use in their work.

When using search engines children will search for specified words only, which have been first checked for suitability by the class teacher. Children will also only use 'safe strict' search under close direction of the Classteacher and for specified purposes only.

Risk Assessment .

- Staff will visit all sites prior to using them with pupils to ensure the material is appropriate for the age range they are teaching.
- Children will be taught e-safety as part of the ICT curriculum.
- The use of computer systems for purposes not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the policy is implemented effectively.

Permissions and Responsibilities .

The parent or guardian of each child will be required to signify their consent to their child/ren accessing the internet at school and according to the provisions in this policy. This follows at the end of this policy.

Although as part of the school curriculum there will be teaching in appropriate and safe use of the internet the school is not responsible for any child's access of the internet outside of school. Parents and Guardians must assume responsibility for their child's internet access whilst at home and are advised to familiarise themselves with procedures and practise designed to assure the safety of minors using the internet.

Monitoring and Review .

Internet use and access is monitored by the Headteacher and ICT subject leader in line with the school policy on monitoring and evaluation.

Staff development needs are identified through appraisal and by means of staff discussion.

This policy will be reviewed annually.

Sept.2019

‘School Name’ Filtering Change Log

All filtering change requests to be recorded by Network Manager or staff member authorised to adjust filtering levels. All filtering changes must be authorised by Head or Designated Person for Child Protection.

Website / category	Date	Requested by / reason	Authorised by	Change made by	Confirmed by	Date for review
www.scribd.com	01/10/10	(AN)Good examples of essay writing. Strong language but is appropriate to age group and in context of literature	Cliff Face (ICT Co-ordinator)	Sarah Mall (ICT HLTA)	Davey Jones (Deputy Head - CPO)	31/10/11

‘School Name’ 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 or Chair of

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)

Dear Parent/Guardian

You will be aware that the internet can provide a valuable source of information in support of many areas of the school curriculum. It is therefore the school's policy to provide internet access to all pupils.

As part of the school policy on the use of the internet, the school has installed provision to filter out material that may be offensive or inappropriate. Children will be taught how to use the internet properly. However these measures can never be totally effective.

Therefore the school cannot take full responsibility for children accessing inappropriate material whilst in school.

In addition the school cannot take any responsibility for pupil's actions whilst using the internet away from school.

In order to give your child access to the internet, the school requires you to give your permission and to indicate that you understand the nature of the school's responsibilities as well as your own responsibilities.

Please read and sign the attached form and return it to the school as soon as possible.

To the parent or guardian of _____

As the parent or legal guardian of the pupil shown above, I grant permission for my son/daughter to use electronic mail and the internet. I understand that pupils will be held accountable for their own actions. I also understand that some material on the internet may be objectionable, that the school has undertaken to eliminate as far as possible the chances of pupils accessing such material and that I accept responsibility for setting standards for my son/daughter to follow when selecting, sharing and exploring the internet.

Parent/Guardian signature_____ Date:___/___/___

Pupil's name_____ Date:___/___/___

Class_____