AKELEY WOOD JUNIOR SCHOOL & NURSERY:
ONLINE SAFETY

Abridged Online safety Policy

1. The online safety policy applies to all staff, pupils, visitors and contractors.

2. The Online Safety Coordinator for the school is Mr M Rice.

3. 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.

4. Websense is used by the school to block and control age appropriate access to content.

5. Staff and pupils receive different levels of filtering.

6. User activity of the school ICT system, including personal use, is monitored.

7. The ICT Technician is responsible for ensuring the infrastructure, network and antivirus software is maintained and secure.

8. Pupils are responsible for signing the Computer Use Agreement, using the Internet safely and reporting any inappropriate materials or conduct.

9. In the case of accidental or intentional misuse, or if staff or learners come across unsuitable online materials, the site must be reported immediately to the online safety Coordinator and/or Head Teacher, when it will be dealt with and logged using the log sheet found at the end of the online safety policy.

10. Online safety is embedded in the ICT curriculum and should be reinforced whenever ICT is used in learning.

11. Pupils must hand in their mobile telephones and devices to the office for safekeeping.

12. Staff may only use mobile telephones outside of lessons and in areas that pupils do not access.

13. Staff are not permitted to use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of students.

14. 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.

15. Parents and carers will be responsible for endorsing (by signature) the Computer Use Agreement.

16. The school will also seek to provide information and awareness to parents and carers through: letters, newsletters, open evenings and other forms of engagement.

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
- 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, 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 telephones or iPads which are brought onto school grounds.

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 Cognita's 'Acceptable Use of ICT, Mobile Devices and Social Networking Sites by Staff' 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 available to all staff and any volunteers, visitors or contractors.

Network Manager/Technical Staff

The ICT Technician, together with Cognita Servicedesk, 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 online safety Coordinator and the Designated Person for Safeguarding.
- that any problems or faults relating to filtering are reported the online safety Coordinator and/or Head Teacher immediately and recorded on the online safety Incident Log.
- that users may only access the school's network through a password protection policy.
- that he/she keeps up to date with online 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 online safety Coordinator.

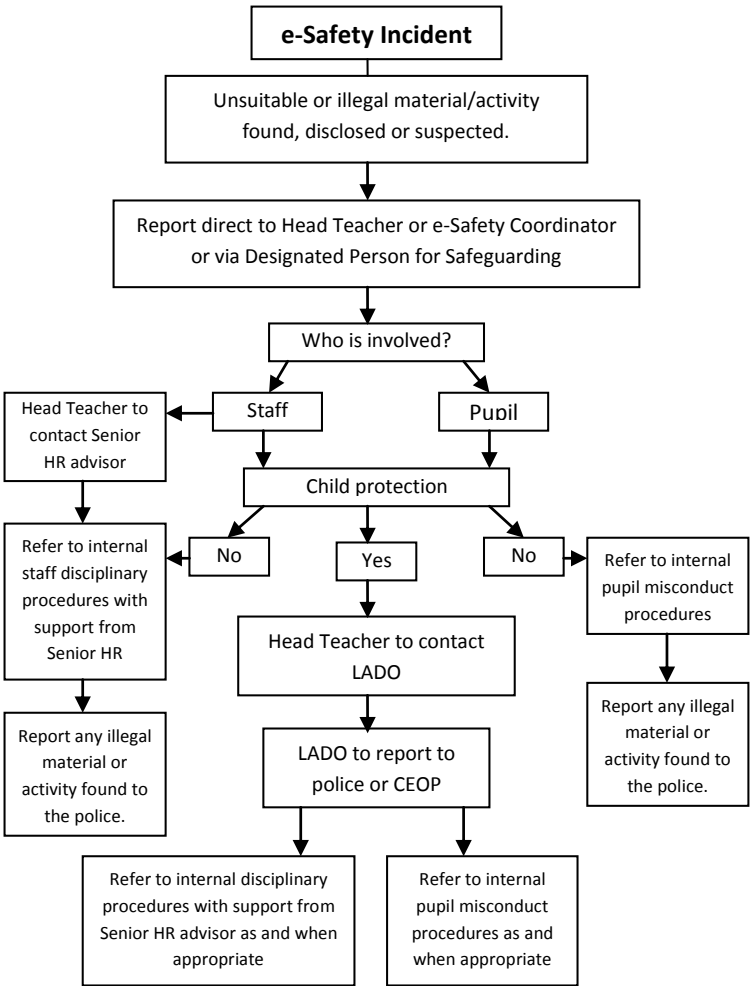
Children and Young People

Children and young people are responsible for:

- Signing agreement to, and abiding by, the Computer Use Agreement for pupils.
- 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 (age dependant)
- Actively participating in the development and annual review of the Computer Use Agreement.

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/online safety Coordinator immediately and the online 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 Cognita.

All incidents must be recorded on the online safety Incident Log to allow for monitoring, auditing and identification of specific concerns or trends. The template can be found at the end of this document. The log is saved on the shared network drive.

Monitoring

School ICT technical staff 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 online safety in all areas of our curriculum and key online safeguarding messages are reinforced wherever ICT is used in learning.

- Pupils are made aware of copyright issues, data protection, intellectual property and reliability of information sourced on the Internet as part of the online 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 online safety issues, including Childline and CEOP

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.

Email Use

Staff

- The school provides all staff with a professional email account to use for all school related business, including communications with children, parents and carers. 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 online safety Coordinator if they receive an offensive or inappropriate email via the school system.
- It is the responsibility of each account holder to keep their password secure and to report any suspected breaches of password security to the online safety Coordinator or ICT Technician. 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.

Students

- 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.

Internet Access and Age Appropriate Filtering

Broadband Provider: BT

All pupils 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:

- Webroot Web Security Service is used by the school to block and control age appropriate access to content.
- Filtering levels are managed and monitored on behalf of the school by our technical support. Upon request, our technical support allows or block access to site and manage user Internet access.
- Staff and pupils receive different levels of filtered Internet access in line with user requirements (e.g. Youtube at staff level but blocked to students)
- Pupils have year group usernames and passwords to access the school network which ensures that they receive the appropriate level of filtering.

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

- Anti-virus and anti-spyware software is used on all network PCs and 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.

Staff

- Expectations for staff online conduct is addressed in the 'Acceptable Use of ICT, Mobile Devices and Social Networking Sites by Staff' Policy
- 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

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the ICT Technician.
- 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.

Mobile/Smart Phones and Devices

Student use:

- Where mobile telephones or devices have been allowed onto school grounds, the device will be turned off and locked away in the School Office at the start of the school day and returned to the student before their homeward journey.

Staff, Parent and Visitor use:

Personal mobile telephones are permitted on school grounds, but should be used outside of lesson time only and in areas where pupils are not present. **No** mobile telephones are allowed in the Nursery setting.

- 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 telephones 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.
- The only exception to this is on trips or in the event of school closure when Form Teachers contact parents to inform them.

Laptops/ iPads

- Staff must ensure that all sensitive school data is stored on the network (shared drive) and not solely on any other 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. 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 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.

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 may 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.
- 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.

Parent/Carer Involvement

As part of the schools commitment to developing online 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 Computer Use Agreement on an annual basis or 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.
- online safety parent/carer sessions are run annually to raise awareness of key Internet safety issues and highlight safeguarding measures in place within 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.

Updated: April 2016
Next Review Date: May 2017

Signed 

Mrs C G Page
Headteacher

Akeley Wood Junior School online safety Incident Log

Details of ALL online safety incidents to be recorded by the online safety Coordinator. This incident log will be monitored by the ICT Coordinator and Head Teacher.

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)