



# Woodseaves CE Academy

## E-Safety & Internet Policy

Pupils have access to the internet and a wide variety of technology with internet access on a daily basis. Although this offers them the opportunity to interact socially and develop their knowledge and learning, they can on occasions be placed in danger.

As a school we must decide on the appropriate balance between controlling access, setting rules and educating pupils to be responsible.

E-safety addresses issues relating to children and their safe use of the internet, mobile phones and other electronic communications technologies, both in and outside of school. It includes education on risks and responsibilities and is part of our 'duty of care' which applies to everyone working with children. Further details regarding Child Exploitation and Online Protection Centre (CEOP) are available online.

### The Purpose of the Policy

This policy is intended to balance the use of educational resources with safeguarding against risks and unacceptable activity. It outlines the terms and establishes the ground rules by which the school provides access to the internet and emails, which must be followed by all users. It demonstrates the methods used to protect the children from sites with unsuitable material. The responsibility for setting and conveying the standards that children are expected to follow is shared with parents and guardians. A combination of site-filtering, of supervision and a responsible attitude in our pupils promotes safe using of the internet to enhance and enrich learning.

### To whom does the policy apply?

The policy applies to all users:

- Governors
- Senior Managers
- Teachers
- Teaching Assistants/support staff
- Others members of staff
- Community users
- Parents
- Pupils

### Using the Internet to Support Teaching and Learning

To enhance teaching and learning opportunities, the internet can provide:

- A wide range of materials for subjects throughout the curriculum
- Opportunities to find current up-to-date information
- Opportunities to communicate with other pupils and teachers
- Development of independent learning and research skills
- Access to global news and world-wide newspapers
- A range of support services
- Virtual visits/exploration
- Access to educational enrichments websites – such as PurpleMash, Abacus etc

## What to be aware of

There is no overall control and censorship of the internet and users must be aware that there is no standardisation of what is acceptable/unacceptable online.

Materials on the internet vary greatly. Some material is biased, inaccurate or misleading (whether deliberately or unintentionally). Internet users must therefore exercise caution in their judgement of what they may find. Children must be encouraged to collect online evidence/information from a variety of sources to ensure more chance of verification.

Pupils must be:

- Protected from obscene material, misuse of drugs, promotion of violence, intolerance, racism and extreme views politically, religiously and socially.
- Taught that they should never give personal information on the internet and that people contacting them may not be who they claim to be.
- Taught the effects and how to deal with cyber-bullying through email/social media.
- Taught that information online can change quickly, information can be added or removed daily.
- Taught not to attempt access to files which they do not have access and should not access other individuals' files.

While educators and parents need to exercise caution in allowing pupils to use the internet, they must not deter them from using it, as the benefits far outweigh the dangers.

As with television and video, parents/carers and educators should and where possible preview material or provide supervision.

## What are the Legal and Ethical Issues?

Schools have the right and duty to monitor the use of the internet and email systems to prevent unlawful use or distribution of offensive material. However, since individuals have a right to privacy, the school must balance this appropriately. To comply with the Data Protection Act 1998 a school must monitor and establish a code giving guidelines on the use of the internet and emails when users use such systems for private communications.

## Use of Information Systems

It is important to review the security of the whole system from user to internet, including essential learning services and personal safety of pupils and staff.

The following measures are used:

- Children are expected to follow specific rules when using the internet; misuse will result in direct action being taken.
- The security of school information systems will be reviewed regularly
- Virus protection will be updated regularly by Concero
- Personal data sent over the internet will be encrypted
- Portable devices must be monitored and managed when used in school
- Files on the school network are regularly checked through Policy Central
- Policy Central records and notifies misuse and possible inappropriate material
- Concero will review system capacity regularly

## Use of the Internet

We undertake the following measures to prevent children from internet misuse and exposure to unsuitable materials:

- Staff are required to sign .....before access is granted
- Pupils and parents are required to sign 'Responsible Internet and E-safety Use' agreement on admission to the school.
- Children are expected to follow specific rules when using the internet; misuse will result in direct action being taken.
- Our internet is purchased from EXA Networks
- Access to the internet is gained via the school network and pupils must have permission from an adult and adult supervision to use search engines.
- Staff must ensure that any videos/images are search for with care and caution and are advised not to do so 'live' within the classroom setting.
- Staff must ensure that pre-selected websites are recommended for pupils to ensure that content is safe.
- Staff are encouraged to regularly discuss with pupils the safety and reliability of the internet.
- Pupils are educated to use the internet safely and responsibly
- Pupils do not have access to emails within school but are made aware of the dangers of communicated via email at home.
- Pupils are encouraged to tell a member of staff immediately if they encounter any material which makes them feel uncomfortable.
- Policy Central records and reports any attempts to access inappropriate sites/material
- Pupils usernames and passwords are accessible to staff and Concero
- The Head teacher will ensure that any new members of staff are provided with the school's policy and ensure that this is followed.
- Policy Central ensures that any inappropriate websites/material sent or received on school laptops whilst being used by staff at home are recorded and reported to school.
- Accessing unauthorised sites is prohibited
- Undesirable sites/web domains/chat groups and social media will be blocked from use.

Disclaimer: Whilst the above measures are designed to help protect children using the internet, they cannot guarantee complete safety.

## Use of Email

At Woodseaves Primary Academy, we use Office 365 to send emails but this is only accessible to staff not pupils. To learn/practise sending/using emails pupils can access simulated sites which allow this to take place securely (such as PurpleMash).

## Published Content & the School Website

The purpose of our school website is to provide information to existing and new pupils and parents. It is also designed to promote the school to prospective parents/pupils.

The following safety measures will be taken:

- Personal information will not be used on the website
- The only point of contact will be the office/head teacher email addresses and the phone number and address of the school.
- Any pupils whose parents do not give permission for their child's photograph to be used with link to the school will not appear on the website.
- Pupils' names will not appear on the website.
- Any text written by the pupils will not be published on the school website before being checked by staff first.
- School will ensure that there is no infringement of copyright published on the school website.
- Any links to external websites will be monitored and regularly checked.
- The Head teacher and Office Administrator are responsible for all content which appears on the school website. The Head teacher will be the point of contact for and queries regarding the website and its content.
- Conzero will regularly monitor the content of the school website.

## Social Networking, Mobile and Gaming Devices

Pupils are not permitted to visit any social networking sites. If this occurs then the head teacher will discuss this with the parents of the child involved. All social networking sites are blocked through our school network sites.

If a member of staff suspects or is informed that a child has been subjected to inappropriate material via social networking/gaming etc at home, this must be logged and the head teacher will contact the parents of the child concerned.

If a member of staff suspects or is informed that a child is using age-inappropriate games (and therefore potential inappropriate content) at home, this must be logged and the head teacher will contact the parents of the child concerned.

Social networking is discussed in KS2 E-safety assemblies and lessons and pupils are advised to:

- Never disclose personal details
- Not place personal photos on any social network site
- Consider how public the information is
- Set up passwords and deny access to unwanted communication
- Invite only friends and deny access to those unknown
- Report any bullying which takes place

Pupils are reminded that they are not to bring mobile phones and gaming devices into school and any found will be removed by the teacher and stored in the school office until the end of the day. The head teacher will be notified and appropriate action will be taken.

## Emerging Technologies

Many emerging communications technologies and websites offer the potential to develop new teaching and learning tools. A risk assessment needs to be undertaken on each new technology and effective practice in the classroom developed. Access will be denied until this has been carried out.

## Safeguarding

In order to make best the use of the many educational and social benefits of new technologies, pupils need opportunities to use and explore the digital world using multiple devices. Adults working in this area must therefore ensure that they establish safe and responsible online behaviours. This means working to local and national guidelines on acceptable user policies.

Communication between pupils and adults, by whatever method should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, emails, digital cameras, videos, webcams, websites and blogs. Adults must not share any information with a child or young person. They should not request or respond to any information with a child or young person other than as part of their professional role. Email or text communication between adults and children outside agreed protocols may lead to disciplinary or criminal investigations. This includes communications via internet websites and social media.

Any photographs taken of pupils must be undertaken using school technology (cameras or ipads). In the event that photos are taken during an off-site visit, this must be also using school multi-media only and not of that owned by the member of staff/adult.

Staff are not permitted access to their mobile devices within the classroom setting and around school – this is limited only to break times/lunchtimes within the staffroom.

Any visitors who will be visiting the classroom areas during the school day, must hand over their mobile devices which will be stored in the school office and only used in the entrance area.

\* If visitors are to be accompanied at all times by the Headteacher/Senior Leader, for example when showing prospective parents around, then they may keep their phone in their bag/pocket but it must be switched to silent.

**Agreed by Governors: June 30<sup>th</sup> 2016**

**Review Date: June 2018**