



Woodgate Primary School

E-Safety and
Acceptable Use Policies

Reviewed by D Carroll & N Malin – October, 2024

Our Vision

Woodgate Primary welcomes the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated communications technologies. However, we are aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. Our schools aims to:

- Have robust processes in place to ensure the online safety of children, staff, volunteers and governors
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance (Keeping Children Safe in Education) available at the following link:

Keeping Children Safe in Education and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

In addition:

- Acceptable Use Policy (AUP) for adults
- Acceptable Use Policy (AUP) for children
- School's behaviour policy
- Anti-Bullying Policy
- Safeguarding Policy.

Publicising e-Safety

To communicate the e-Safety Policy we will:

- Make this policy, and related documents, available on the school website at: [woodgateprimary.co.uk](https://www.woodgateprimary.co.uk) through our dedicated e-Safety page;
- Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated;
- Post relevant e-Safety information in all areas where computers are used.
- Provide e-Safety information at parents' evenings and through the school newsletter, website and Xpressions.

Roles and Responsibilities.

Head Teacher: **Mrs D Colley**

Designated Safeguarding Lead: **Miss D Carroll**

ICT Manager: **Mr D Grey**

Lead Governor E Safety: **Mrs S Barratt**

Governing Body.

The governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL). All governors will ensure that they have read and understand this policy.

The Designated Safeguarding Lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, ICT Manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged on "My Concern" and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing annual report on online safety in school to the headteacher and governing body.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

The ICT Manager

The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
-

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged on My and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Not having their personal mobile phones on when children are present.

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? - UK Safer Internet Centre Hot topics – [Click here](#)
- Childnet International Parent factsheet – [Click here](#)
- Childnet International Healthy relationships – Disrespect Nobody – [Click here](#)

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety Pupils will be taught about online safety as part of the curriculum.

Physical Environment / Security

The school endeavours to provide a safe environment for the whole community, reviewing both physical and network security regularly, monitoring who has access to the system and consulting with the LA where appropriate.

Anti-virus software is installed on all computers and updated regularly.

ENTRUST: the school internet activity is monitored by Entrust at all times. The Head Teacher, Deputy Head Teacher and School Business Manager receive alerts if there are 'captures' of inappropriate content. These are graded according to severity. These alerts are responded to in a timely manner. Many are 'false positives.' Where there is a concern this is followed up and recorded on My Concern.

All staff are issued with their own username and password for network access.

Visitors / Supply staff are issued with temporary ID's and the details recorded in the school office.

Reception and Key Stage One pupils will use class logon ID's for their network.

Key Stage Two pupils have their own username and a class password. Mobile / Emerging Technologies.

Educating pupils about online safety

The education of pupils in e-safety is an essential part of the school's e-safety provision. At Woodgate we recognise that children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- A planned e-safety programme is provided as part of Computing / PHSE / and other lessons and should be regularly revisited - this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies or lessons; Pupils should be helped to understand and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils will be advised never to give out personal details of any kind, which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends/family, specific interests and clubs etc...

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home and in information via our website or Expressions. This policy will also be shared with parents. Online safety will also be covered during parents' evenings. Workshops to raise awareness of internet danger will be offered to parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm
- Disrupt teaching
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or retain it as evidence (of a criminal offence or a breach of school discipline), or report it to the police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3).

Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

Children using mobile devices in school

Before children bring their mobiles to school there must be a signed parental agreement in place. Children may bring mobile devices into school, if they walk home on their own, but are not permitted to use them during the school day. They are locked away in the office and returned at home time. They are not allowed to turn on their phone until after home time.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, ICT and acceptable internet use.

The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.

They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.