



GREENBANK PREPARATORY SCHOOL & DAY NURSERY

Policy for Internet Usage and E-Safety

Member(s) of Staff Responsible	Adam Dyson
Date of Current Policy	Spring 2019
Date to be Reviewed	Spring 2020

‘Greenbank aims to provide a caring environment where traditional values of courtesy, respect for others and pride in work enables all children to develop their talents, gain self-esteem and reach their full potential.’

This is a whole school policy which includes the Early Years Foundation Stage, which is the Nursery, Preschool and Reception classes. This policy should also be read in conjunction with the School's Safeguarding Policy.

Rationale

Use of the Internet is continually expanding and has become an important part of learning and communication. The Internet brings pupils into contact with a wider range of information, the scope and nature of which may or may not be appropriate for the pupil. The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT. When distributing the curriculum, teachers need to prepare for and make use of communications technology i.e. web-based resources and email.

The Internet is managed by a worldwide, non-statutory collaboration of independent agencies that serve both young and adult audiences. Without appropriate measures, access to unsuitable materials would be possible and security compromised.

This Internet Usage Policy will help to ensure that Internet supports school's educational aims, that responsibilities to pupils are met and that safety and security requirements are satisfied.

The appropriate use of the Internet provides a number of benefits to schools. These benefits include:

Resources

- Providing access to documentation including on-line publishing of documents (schools' policies, lesson plans, activities, etc)
- Access to world-wide educational resources including museums and art galleries
- Inclusion in government initiatives
- Information and cultural exchanges between students worldwide
- Discussion with experts in many fields for pupils and staff Professional Development
- Sharing good practice with colleagues
- Communication with the advisory and support services, professional association and colleagues

The school's Internet Usage Policy complements the school's **computing** policy and relates to other policies including those for behaviour, citizenship and personal, social and health education (PSHEE).

Aims

The aim of this document is to ensure that the following goals are understood:

- To ensure staff and pupils use the Internet safely and effectively
- To put in place measures to protect school from undesirable content
- To raise awareness of staff and pupils to the benefits of Internet access

Objectives

- To develop strategies to use the Internet
- To encourage suitable use through education and guidance.
- To promote the use of the Internet as a learning tool.
- To promote safe and useful learning through the Internet.

Implementation

Teachers, parents and pupils need to develop good practice in using the Internet as a tool for teaching and learning. With systems in place to minimise the risk of inappropriate material being viewed, pupils will be able to select resources independently. Over time they will develop greater skill in determining which material is appropriate and of good quality, as well as whether or not it is a better source than other media, such as good books. Internet access within Greenbank Preparatory School provides a service designed for pupils. This includes filtering appropriate to the age of pupils.

How will the Security of School ICT Systems be maintained?

Greenbank Preparatory School has put in place a system of logins that encourages users to be responsible for their own Internet access. It is essential that users – both staff and pupils - log out, and this needs to be reinforced as good practice whenever possible. Maintaining security of the school systems is of paramount importance as sensitive data is stored within it. Greenbank Preparatory School provides an individual username and password for each user to log onto the network. Through their own account they then have access the internet. Our SmoothWall filter can provide detailed information of a user's activity. Users are made aware of the importance of logging off at the end of a session and staff always lock their computers or log off should they be leaving their equipment unattended. Maintaining security of the school systems is of paramount importance as sensitive data is stored within it.

How will the school ensure Internet Access is Safe?

Access to appropriate information should be encouraged and Internet access must be safe for all members of the school community from youngest pupil to teacher and administrative officer.

With respect to using the school's Internet provision, various strategies are used to try to ensure staff and pupils are protected. It is important, however, to understand that none of these systems can be completely effective in isolation therefore a combination of approaches is used:

Trustees will ensure that:

- All staff have been given the opportunity to discuss the policy
- The policy is ratified and reviewed as necessary

The School will ensure:

- Authorised users are given a unique username and password. Authorised personal will be required to change their password once a school year.
- Teaching staff will be given a Greenbank email account via Office 365. The password will be refreshed every three months.
- Rules for Internet access are posted near computer systems.
- Staff are given opportunities to discuss the issues associated with Internet access and develop appropriate teaching strategies
- New facilities are thoroughly tested before pupils are given access

- Filtering software is used to block websites deemed inappropriate, using a number of lists or categories of URLs that can be marked as allowed or denied. These lists are updated frequently by our SmoothWall filter.
- Greenbank's firewall (Smoothwall) is regularly checked. Hard copies of updates are printed and saved within a folder in the server room which is managed/checked by the computer coordinator.

Staff will ensure that:

- Pupils are never sent to work on computers with Internet access without a member of staff being present in the room
- Sites being used by pupils are monitored during lessons, as the nature of the internet is such that children will easily move from one site to another without even being aware
- They are aware of the possibility of inappropriate adverts or pop-ups on sites such as YouTube
- Access to inappropriate content is reported to the Headteacher as soon as possible.

Along with the strategies outlined within this policy for safe Internet usage at school, Greenbank also issues guidelines for safe Internet usage at home. This includes both recommendations for parents as well as a contract for children to sign to acknowledge that they understand some of the possible risks. These contracts differ from KS1 to KS2 and are outlined at the end of this policy along with the recommendations to parents.

Misuse of the internet

If a child is found to be misusing the internet whilst on school grounds or whilst using Greenbank Preparatory school devices. He/she will have all access to the internet removed in school for one term and parents will be informed. After one term the headteacher will review each case and decide if access should be returned or if a further consequence should be implemented.

Special Needs, Exceptionally Able and Talented

The Internet can be a positive tool for children with Special Educational Needs.

Access to the Internet is therefore a vital link with which communication to the outside world can be achieved. Access to the Internet can also stimulate children to develop their ideas and research independently.

Equal Opportunities

Access to the Internet is a necessary tool for all staff and students irrespective of gender, race, religion, culture or ability.

Resources

It is expected that resources will be used from the Internet for teaching and learning materials. It is vital schools acknowledge the origination of resources, authenticate the author, examine the target audience and discriminate between what is fact and fiction.

The following separate policies, available on request, should be read in conjunction with this policy.

- Social Media Policy
- Acceptable Use Policy
- Cloud Storage Policy
- Cyber-bullying policy



Tips to help keep children safe on the internet

Preventing your children from using the internet or mobile phones will not keep them safe in the long run, so it is important to have conversations that help your child understand how to stay safe and what to do if they ever feel scared or uncomfortable. Below are 6 easy first steps to help parents maintain a standard of e-safety both in school and at home.

6 easy steps to help keep your children safe online

Controls are not a single solution to staying safe online. Talking to your children and encouraging responsible behaviour is critical; however controls are a vital first step to helping to protect your child online.

1. Set up home broadband parental controls

These allow you to control what content is seen on any device connected to your broadband router or hub.

2. Set controls on your search engine

Encourage your child to use child-friendly search engines, and activate and lock safe search settings.

3. Make sure every device is protected

Controls should be installed on every device your child uses – mobile phones, tablets and games consoles.

4. Privacy settings

Activate safety measures offered by different sites. Sites like Facebook have settings that help prevent your child seeing unsuitable advertising.

5. Block pop-ups

If you are worried about your child accessing inappropriate content through clicking on pop-ups, BBC Webwise has advice on how to stop these.

6. Keep talking

Parental controls are a really useful part of your toolkit in keeping your child safer online and they can be adjusted as your child grows; however it is vitally important to remember to talk regularly to your child about what they are doing online.

You can find more tips on how to start these conversations at [**internetmatters.org**](https://internetmatters.org).

1. EYFS

Think then Click

These rules help us to stay safe on the Internet.



We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.



We always ask if we get lost on the Internet.

We tell an adult if we see something we don't like or understand.



We can send and open emails when an adult is present.

We never give out personal information – name, address, school, or anything!



We never give out password information – even to a friend.

I have read through this with my child

Signed Date:.....

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet.



We only use the internet when an adult is with us.

We can click on the buttons or links when we know what they do.



We always ask if we get lost on the Internet.

We tell an adult if we see something we don't like or understand.



We do not hang around in a chat-room if anyone says anything which makes us feel uncomfortable. We report this to an adult.



We can send and open emails when an adult is present.

We can write polite and friendly emails to people that we know.



We never give out personal information – name, address, school, or anything!

We never give out password information – even to a friend.

We never arrange to meet anyone we don't know.

Signed (child)..... Date:.....

Signed (teacher)..... Date:.....

Signed (parent)..... Date:.....

Key Stage 2

Think then Click
e-Safety Rules for Key Stage 2 (at home AND at school)
• We ask permission before using the Internet. • We tell an adult if we see anything which makes us feel uncomfortable. • We immediately close any webpage we are not sure about. • We only e-mail people an adult has approved. • We send e-mails that are polite and friendly. • We do not upload pictures of ourselves without agreeing it with our parents first. • We tell an adult if we get an e-mail from anyone we don't know. • We never give out personal information – name, address, school, or anything! • We never give out password information – even to a friend. • We never arrange to meet anyone we don't know. • We do not hang around in a chat-room if anyone says anything which makes us feel uncomfortable. We report this to an adult. • We never enter our email address into a web page without checking with an adult first. • We understand that our emails may be read / checked by an adult – a parent or a teacher

Signed (child)..... Date:.....

Signed (teacher)..... Date:.....

Signed (parent)..... Date:.....