

Introduction

This policy outlines our purpose in providing e-mail and access to the Internet at Greenhill Primary School and explains how the school is seeking to avoid the potential problems that unrestricted Internet access could give rise to.

Internet access in school

Providing access to the Internet in school will raise educational standards and support the professional work of staff.

Teachers will have access to the Internet offering educational resources, news and current events they will also be able to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA and DFE. The Internet is being used to enhance the school's management information and business administration systems.

Pupils will have access to the Internet offering educational resources, news and current events. There will be opportunities for discussion with experts in many fields and to communicate and exchange information with students and others world-wide. All staff (including teachers, supply staff and classroom assistants) and any other adults involved in supervising children accessing the Internet will be made aware of the Acceptable Use Policy and will have its importance explained to them. Parents will be drawn to the Policy through the school website

Using e-mail

All staff are strongly advised **NOT** to use or share their personal email account for school and therefore are issued with their own professional email which they will use appropriately to communicate with colleagues and schools external services.

Pupils will learn how to use an e-mail application:

- Once they have been taught about Acceptable Use and agreed to their Acceptable User Policy responsibilities
- Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Pupils will not be permitted to use e-mail at school to arrange to meet someone outside school hours.

Internet access and home/school links

Parents will be informed that pupils are provided with supervised Internet access as part of their lessons.

E-Safety will be taught to all pupils from Reception (at an appropriate level) and will be readdressed every year. Sessions will be taught using age appropriate resources and cover the following areas:

Email, SMS Messaging, Social Networking and Cyber Bullying. All children within these sessions will have the opportunity to agree to their own Acceptable Users Policy.

If a reported incident arises outside of school, staff will log the event with the Computing Co-ordinator, and where necessary, parents will be informed and a discussion to take place with all parties. In serious cases it will be referred onto the designated teacher for Safeguarding and/or the MASH team.

Social Networking

Online social networking and interactive services can provide extensive benefits to their users. However while staff and volunteers will want to make the most of these services, this document aims to ensure they understand the importance of protecting themselves, their online identities and their reputations. It is vital that staff / Governors/volunteers are aware of the importance of keeping

private and professional information separate. Irresponsible use of new technologies can affect your reputation, your self-esteem, your health and, in some cases, your career progression.

Social networking sites include, amongst others:

- Facebook
- Bebo
- LinkedIn
- MySpace
- Twitter

Security Settings

It is vital that when you register to become a user of a social networking site, you ensure that you access the 'settings' page and set security to their highest possible level. This will ensure that only those people who you authorise to see your information will be able to see it, however remember that friends may respond to your comments, or post comments on your photographs which their friends are then able to see, and so on.

Friend Requests – Sending and Receiving

Under no circumstances must staff/Governors/volunteers accept friend requests from children who do or have attended Greenhill Primary or have had professional contact with; nor should they make such requests. Should a young person attempt to contact you in this way, you should make this known to your manager immediately.

Remote access to social networking sites

Many staff/Governors/volunteers and young people now have the facility to access their social networking information 'on the move' and can keep it updated at all times via mobile phones, iPads etc. It is vital that these items are password protected to the highest level to avoid unauthorised access/use.

Social Networking Dos and Don'ts

Do

- Think about who you want to see your personal information
- Read the privacy settings information carefully
- Set your profile to private/the highest security setting
- Review your 'friends' list regularly to ensure you still want them to know your personal details
- Think very carefully about what you share with friends, even if your information is 'private' as this may appear on your friends page
- Protect your password and never share it with anyone else
- Only communicate with pupils via official school systems
- Be careful about the kind of information (including images) you share about yourself and how you manage your online reputation. Other people can pass on or change your information and you might not be able to stop them or delete it afterwards
- Use a strong password – numbers as well as letters, upper and lower case, and never let anyone else have it

Don't

- Share information that shows you or your friends in a compromising situation
- Post content that may be seen as racist, homophobic, bullying or threatening
- Bring the school into disrepute by posting derogatory comments about your work/employer
- Use personal equipment, i.e. mobile phones or cameras to take photographs of children and young people
- Give any personal details, including your mobile number, to a young person.

Using information from the internet

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that, unlike the school library for example, most of the information on the Internet is intended for an adult audience, much of the information on the Internet is not properly audited/edited and most of it is copyright.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true
- When copying materials from the Web, pupils will be taught to observe copyright
- Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed. If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will wish to respond to the situation appropriately and in line with Policy
- Staff will log the event with the Computing Co-ordinator/designated teacher for Safeguarding and Headteacher
- A letter will be sent home to inform parents

Maintaining the security and safety of the school network

We are aware that connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or accessed by unauthorised persons.

- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils
- Staff will be particularly vigilant when pupils are undertaking their own search and will check that the children are following the agreed search plan
- Staff will ensure that when searching the Internet for images that all projectors and Smartboards are turned off
- If staff or pupils discover unsuitable sites the Computing co-ordinator will be informed. The URL (address) and content will be reported to the Apex support team
- If it is thought that the material is illegal, after consultation with the Computing Coordinator and Apex support team, the site will be referred to the Internet Watch Foundation and the police
- A child friendly Acceptable Use and E-Safety poster will be posted in all classrooms

It is the experience of other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the Internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. Neither the school, Bury LA nor Apex can accept liability for the material accessed, or any consequences thereof. A most important element of this and our Acceptable Use Policy is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.