Woodfield Primary School

E-Safety & Acceptable Use Policy

Document Approval

This document was reviewed and approved by the Governing Body as appropriate and effective.

Signed:		
Date:	21/11/2016	21/11/2016
Name:	Mrs L Porter	Mrs J A Charnley
Position:	Chair of Governing Body	Headteacher

Document Review

The Governing Body will review this policy to ensure that it is appropriate and effective whenever necessary, and not less than once every three years.

Document Control

There is one controlled paper copy of this document located in the Business Manager's Office.

The master electronic copy is held within a designated folder. The latest issue will be marked with the highest number, ie Issue 2 is later than Issue 1. Files in the process of being edited have the words 'In Progress' in the file name.

All other copies (electronic and paper) are uncontrolled.

Document History

Filename: E-Safety & Acceptable Use Policy				
Issue	**Description of Change**	**Author**	**Checked**	**Date**
1.0	Reviewed and agreed by staff/ approved by governors.	JAC	SB	26.07.2011
2.0	Reviewed – November 2013	JAC	SB	Nov 2013
3.0	Reviewed – November 2016	JAC	SB	Nov 2016
4.0	Review date – November 2019			

Woodfield Primary School
Wigan Lane
Wigan
WN1 2NT

Telephone: 01942 243675
E-mail: enquiries@admin.woodfield.wigan.sch.uk
Web: www.woodfield.wigan.sch.uk

1 Introduction

1.1 At Woodfield, we exercise caution when allowing children access to the IT, as we recognise there are risks. However, we encourage the use of IT as we believe its educational benefits outweigh any possible dangers. Schools have always helped learners to engage with society based on clear support and guidance, and in our school the use of the internet and related technologies is no exception.

1.2 As with any media, our clear policy is for staff to preview material or provide supervision. This is in addition to the commonsense steps (described below) for ensuring children's safe use of the internet.

1.3 We use a filtered broadband service, which meets the government guidelines for blocking material that is inappropriate for primary school children. However, we make it clear to our parents that it is not technically possible to block access to all inappropriate or controversial material, which is why we take the steps outlined in this policy.

1.4 We minimise the risks of using the internet and related technologies by taking the following commonsense steps:

i. We encourage and support our staff in training and continual learning in IT.

ii. We position computers in public places where everyone can see what is on the screen.

iii. We take an interest in the internet and regularly discussing what young people see and use.

iv. Our staff are aware of what research projects children are carrying out on the internet.

v. We monitor the amount of time children spend online at school and we avoid excessive hours spent on the internet.

vi. We educate our children to use the internet in a sensible and responsible manner.

vii. We encourage children to be critical users of the internet, asking questions such as: 'Is the information true? How do you know?'

viii. We warn children that there are some unsuitable sites on the internet and discussing the issues involved.

ix. We warn children that there are some people (adults) who use the internet (including email, chat rooms and instant messaging) and mobile 'phones to forge friendships with children in order to either lure them into meeting, or to trick them into disclosing information that allows them to be identified. We explain that these people do this as they want to hurt or bully children and we discuss the issues involved.

x. We ensure children know what to do if they find upsetting material.

xi. We share details of our E-Safety & Acceptable Use Policy with parents and seek their support in providing consistent messages to our children.

xii. We discuss and agree the school computer rules with children in class.

2 Appropriate Use of School IT Equipment

2.1 At Woodfield, IT equipment (computers, laptops, digital cameras, projectors, etc) is primarily used for educational purposes only.

2.2 For staff, this will include teaching, preparation, administration and other aspects directly connected with the smooth operation of the school and the teaching of our children.

2.3 For children, use will mainly be limited to lessons as directed by teachers.

2.4 The school's IT equipment may on occasion be used by the community, with the permission of the head teacher. In this case, special user access will be granted that does not allow any access to staff or pupil data.

2.5 All uses of the school's IT equipment shall comply with the following:

i. only use the IT equipment for the school/educational purposes, unless specifically agreed by the Headteacher;

ii. virus scan files introduced via CDs, memory sticks, etc.;

iii. don't load or install programmes or applications;

iv. don't access inappropriate or offensive material;

v. don't post/send inappropriate, offensive material; and

vi. don't alter or change the settings or configuration, unless directed to be the technician or help desk.

2.6 The penalties for misuse of school IT equipment are serious. Pupils and other users may be banned from having further access and pupils may face additional disciplinary action as deemed appropriate by the Headteacher.

2.7 Staff who misuse the school's IT equipment will face formal disciplinary action.

3 Appropriate Use of Email

3.1 All staff have school email accounts for school use. Pupils at our school have individual and class/group email accounts which are used as part of IT teaching; the teacher controls the access to the class email account.

3.2 The school's email service includes spam and virus filtering. This minimises the risk of receiving spam and inappropriate or offensive material via email, but it impossible to guarantee that such material will not get through.

3.3 If spam or inappropriate/offensive material is received via email it should be reported to the School Business Manager.

3.4 All email users are warned to be wary of emails received unexpectedly, or from a sender who is unknown to them. Email is a common source of viruses – especially via attachments. Email users know not to open (double click) of attachments received unexpectedly, or from a sender who is unknown to them. Suspicious emails should be reported to the School Business Manager.

3.5 All email users are aware of the insecure nature of email and confidential pupil data is not sent via email.

3.6 All school email accounts are accessible via Office 365.

3.7 The penalty for misuse of the school's email facilities are serious. Pupils and other users may be banned from having further access, and pupils may face additional disciplinary action as deemed appropriate by the head teacher.

3.8 Staff who misuse the school's email facilities will face formal disciplinary action.

4 Other Services and Emerging Technologies

4.1 We constantly monitor the use our children make of new services and emerging technologies, and we consider the affect these have on their education and safety.

4.2 The governors and staff carefully consider government and local authority guidance, and our local community in order to build in mechanisms for incorporating other technologies within the acceptable use policy as they emerge.

5 Protecting Pupils

5.1 In order to protect the identity of our children, we will not include material on our website that allows a child's photograph to be linked to their name or any other personal information.

5.2 In order to protect our children, we no not allow children to have access to chat rooms or instant messaging services in school.

5.3 In order to protect our children, and in this interests of removing distractions from the classroom, we do not allow children to have mobile phones in the classroom.

5.4 We teach children about internet safety and we discuss with them the school internet safety guidelines.

5.5 We teach children about internet safety and etiquette as part of our on-going anti-bullying initiatives.

5.6 We provide information to help educate and support parents about internet safety. We work with parents to with the objective of providing our children consistent messages about internet safety.

6 Protecting Resources

6.1 Our IT equipment and resources are managed and maintained by an external, professional organisation – IT service providers, Benchmark North (Ltd).

6.2 Benchmark North (Ltd) are responsible for ensuring our systems have the latest patches and virus protection. They advise us on any other measures that we should put in place to maintain the security, availability and reliability of our IT equipment.

6.3 The data held on our IT systems is backed up daily and the back-up facility checked and exchanged weekly by the IT Technician from Benchmark (North) Ltd.

7 Passwords

7.1 All users of the school IT system need a username and password to gain access. This username and password can only be used to access the system via a computer in the school; our school currently does not permit staff or pupils to access information stored on the school IT system when they are away from school.

7.2 Staff should change their password regularly to maintain security of their accounts, which provide access to sensitive information.

7.3 Pupils do not have the ability to change their password and a record of their password is held by the class teacher.

7.4 The passwords for common/shared usernames (i.e. the infant class username and guest username) are changed periodically.

7.5 The passwords and usernames used to access email accounts via Office 365 are different to those used in school to access the IT system. Office 365 account passwords are changed periodically.

8

9

10 Legal Considerations

10.1 Certain behaviour is clearly illegal such as using a computer to perpetrate credit card fraud, to spread viruses, to hack into other computers, or to download copyrighted materials. Such issues are covered by the Computer Misuse Act 1990, the Data Protection Act 1998 and copyright legislation.

10.2 All adult users of our school IT equipment are made aware that the use of any equipment, system, network or account for any form of illegal activity is strITly forbidden.

10.3 We take steps in our lesson planning to teach our children about what is right and wrong. We work through methods of preventing them, or strategies for dealing with them should they arise.

11 Sanctions

11.1 Our school will employ appropriate and fair systems for dealing with deliberate misuse of computer systems, both internal and external.

11.2 Depending on the seriousness of the offence, internal sanctions might range from first warnings to temporary bans from using the IT resources, to involvement of parents and guardians and in extreme cases, permanent exclusion.

11.3 Most offences are likely to be pupils simply playing around, to see what they can do. For more serious violations, it may be necessary to involve the police.

9.4 We currently utilise “Securus” software to monitor computer activity in school by parents and pupils.

12 Promoting and Maintaining Awareness

12.1 The acceptable use policy is available on VLE and referred to in the school prospectus. It is also provided to all new staff who join the school and displayed in the IT Suite and classrooms.

12.2 We ask parents to sign a permission form when their child starts school, where they agree to support these rules and accept that our policies and procedures mitigate the risks involved with internet and computer use to an extent where the benefits outweigh the risks.

13 Acceptable Use of IT at Home

13.1 Although acceptable use policies are a little formal for home use, our parents are encouraged to discuss and agree some sensible points with their children. Sensible steps include keeping in touch with what children are doing with their computers, by asking them to show which sites they have visited and talking about what they learned there.

13.2 Talking to children about what is, and what isn’t, acceptable use of the internet will help them to form balanced opinions and set standards that they will apply to any new material they meet, whether at home or at school.

13.3 If parents want support or advice, they are encouraged to talk to staff at any time. We regularly advise parents of links to useful websites.

14 Further Information

14.1 We have relied heavily on the following Government websites in developing this policy:

- http://stagesafety.ngfl.gov.uk/schools/document.php3?D=d56
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet/