Woodmancote School
Belong · Aspire · Achieve

Acceptable Use Policy

Designated member of staff: S Perkins/D DeGruchy

Contents

1 Introduction

Information Technology (IT) in its many forms (eg the internet, email, laptops, tablets and digital recording devices) are an important aspect of our daily lives. Consequently, Woodmancote aims to embrace the use of these technologies in order to help develop the skills our children will need to access life-long learning and employment. We aim to make all users (ie staff and pupils) of the technology (both fixed and mobile) that school provides aware of the risks so it can be used safely.

Disclaimer: *Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.*

Woodmancote School's networked resources, including the internet, email, SIMs, Target Tracker and Class Dojo, are intended for educational purposes, and may only be used for legal activities consistent with our school rules. Any use of the network that is either illegal or would bring the name of the school or County Council into disrepute is not allowed. As such, this policy sets out the conditions that all uses are required to follow. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

2 CONDITIONS OF USE

Pupils

Where the user is a child, or young person, the behaviour while using the technology will be the responsibility of the supervising adult. However, children will be expected to use the technology appropriately and safely (see also guidance contained in the E-Safety policy). This will be demonstrated by pupils, in discussion with their parents or guardians (and reinforced by staff), by signing the Conditions of Use for Pupils (see Appendix 1).

Staff (& or Governors, parents or visitors)

Where the user is an adult, they will be expected to use the technology for the purposes for which they have been made available. It is the responsibility of the User to take all reasonable steps to comply with the conditions set out in this policy. This will be demonstrated by agreeing to, and signing the 'Conditions of Use' (see Appendix 2).

3 Roles and Responsibilities

Governors, Head and Senior Leaders

As eSafety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named eSafety co-ordinator in our school is Samantha Perkins and Duncan de Gruchy.

Senior Leaders, Staff and Governors are updated by the Head/eSafety co-ordinator to all have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy is also linked to the following mandatory school policies: child protection, health and safety, behaviour (including the anti-bullying) and data protection policies.

E-Safety Coordinator

It is the role of the eSafety co-ordinator to keep abreast of current issues and guidance through organisations such as SWGFL, Becta, CEOP (Child Exploitation and Online Protection) and Childnet. Links to current guidance is referred to in Appendix 7. All members of the school community will be made aware of who holds this post.

The E-Safety coordinator will be responsible for sharing school's expectations in this policy and update this as necessary through staff meetings, training, continuing professional development or documentation provided to inform short term users such as visitors or supply teachers. New staff receive information on the school's acceptable use policy as part of their induction.

The E-Safety coordinator, and members of the SLT, will periodically review that the Conditions of Use agreements (Appendix 1 & 2) are signed by all current users.

All Users

It is the responsibility of all Users to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will also accept personal responsibility for reporting any misuse of the network to the eSafety coordinator, or another member of senior staff.

4 Managing infrastructure & internet

- School internet access is controlled through the **South West Grid for Learning** (SWGfL) filtering tool (RM SafetyNet). This ensures unsafe, illegal or inappropriate content is filtered. All use of SWGfL is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.
- In certain circumstances, and only for valid educational reasons that do not compromise school rules or the ethos of this policy, access to sites or software that requires the filter levels to

be lifted can be granted. This will only occur where the Conditions of Use for adults (Appendix 2) has been understood and signed.

- In no circumstances will this be granted to pupils or young people.
- As part of the computing curriculum, pupils will be taught how to identify safe, illegal or inappropriate content and know how to report it. Similarly, staff will have training so they know how to identify the risks and how to report them.
- The school maintains students will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Staff will ensure children are safe from terrorist and extremist material when accessing the internet.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs, social media and instant messaging.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the e-safety co-ordinator.
- It is the responsibility of the school to ensure that Anti-virus protection is installed on all school machines. This automatically updates.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.
- If there are any issues related to viruses or anti-virus software, the e-Safety co-ordinator should be informed.

5 Managing passwords & data

- All users will be provided with an individual login username. Staff will also be given a password to access the school internal server.
- All users need to create secure passwords (ie which are at least 8 characters and include a capital letter, number and special character – eg *, #, ! etc).
- Passwords to networked resources shared by groups of users will be changed periodically, at least annually, to ensure security is not compromised.
- If any user suspects their password has been compromised, they should report it as soon as possible to the e-Safety coordinator to take steps to reset it.
- No Users are allowed to deliberately access files on the school network, of their peers, teachers or others.
- Any confidential data, or personal details will be stored in a password protected device or storage system (refer to Data Protection Policy).

5 Managing emails

- Woodmancote School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Woodmancote uses Office365 to provide all staff with an email account to be used for all school business to reduce the risk of unsolicited or malicious emails.

- Staff should not use their own personal emails to make contact with parents, pupils or other professional bodies.
- It is the responsibility of the account holder to keep their passwords and content secure.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder. An example is attached as an appendix to this policy (see Appendix 3)
- Emails sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform (the eSafety co-ordinator/ line manager) if they receive an offensive e-mail.

7 Managing digital recording devices

- Woodmancote School recognises the value of taking, publishing and storing images and sound recordings to support teaching and learning, however it also recognises that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.
- Permission to use images of pupils, or their work, is sought on a child's entry to Woodmancote by signing the relevant section on the Admissions form. This consent is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc. Parents/guardians may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.
- Records of these permissions are kept on the school management information system (SIMs).
- Images and recordings are permitted to be used in the following ways:
  - on the school web site
  - in the school prospectus and other printed publications that the school may produce for promotional purposes
  - recorded/ transmitted on a video or webcam
  - in display material that may be used in the school's communal areas
  - in display material for use in external areas, ie exhibition promoting the school
  - general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Storage of Images

- Images/ videos of children are stored on the main server.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g USB sticks) without the express permission of the Headteacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

8 Managing mobile devices

Emerging mobile technologies (such as tablets and smartphones) will be examined for educational benefit and the risk assessed before use in school is allowed. Woodmancote school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

8.1 Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- No images or sound recordings of any pupils or young people are permitted to be stored on these devices.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

8.2 School provided Mobile devices (including phones)

- Where the school provides mobile technologies such as phones, laptops for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- Where the school provides mobile technologies such as laptops or tablets for a pupil's personal educational use an agreement needs to drawn up about its terms of use and the responsibility of its care and maintenance between Woodmancote School and the parents or guardians. An example is attached (see Appendix 4).

9 Reporting Incidents

- Complaints about the misuse of any hardware or network resources provided by the school should be made to the eSafety coordinator or the Headteacher. Incidents should be logged (eg on a record sheet such as Appendix 5) and appropriate action taken. See Flowcharts for Managing an eSafety Incident (Appendix 6).
- Where deliberate access to inappropriate materials by any user leads to criminal activity or is of a child protection nature, the incident could be reported, to the police. Immediate suspension or possibly dismissal could follow.
- Users are made aware of sanctions relating to the misuse or misconduct on the Acceptable Use Agreement

This policy should also be read with reference to the following supporting policies:

- Safeguarding
- Data Protection
- E-Safety

Reviewing this Policy

Review Procedure
There will be an on-going opportunity for staff to discuss with the eSafety coordinator any issue of eSafety that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Date: October 2015

Signed…….. (Chair of Teaching and Learning)
Review: October 2016

Appendix 1

Woodmancote School

Dear Parent/ Carer

Computing including the internet, email and mobile technologies, etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Samantha Perkins or Duncan DeGruchy.

✂---

Parent/ carer signature

We have discussed this and …………………………………………..(child name) agrees to follow the eSafety rules and to support the safe use of ICT at Woodmancote School.

Parent/ Carer Signature …………………….………………………….

Class …………………………………. Date ……………………………

Woodmancote School
Belong · Aspire · Achieve

Appendix 1 continued

Acceptable Use Agreement/e-Safety Rules for Pupils

Pupils that do not follow these rules may find:

- They can only use the computers if they are more closely watched.
- They are not allowed to use the computers
- They are excluded from school

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use polite language when using the computers I must not write anything that might: upset someone or give the school a bad name.
- ✓ I know that my teacher will regularly check what I have done and if they think I have been breaking the rules can check how I have been using other IT resources
- ✓ I will only use the school email address when emailing.
- ✓ I will only open email attachments from people I know, or who my teacher has approved.
- ✓ I will not tell my username and passwords to anyone else but my parents I must never use other people's usernames and passwords, or computers left logged in by them.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/guardian will be contacted if a member of school staff is concerned about my eSafety.
- ✓ I will report any websites that make me feel uncomfortable or unsafe to a member of staff.

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)
Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.
Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'
Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online
Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Woodmancote School
Belong · Aspire · Achieve

Appendix 2

Woodmancote School Acceptable Use Agreement for Staff, Governors and Visitors

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school eSafety coordinator.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- I will only use the school's email/Internet/Internal network/and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS or Target Tracker) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without seeking permission from the Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of Computing and related technologies.

User Signature

I agree to follow this code of conduct and to support the safe use of COMPUTING throughout the school

Signature ……Date ……

Full Name ……(printed)

Appendix 3

Example of a disclaimer to be added to email messages sent on behalf of school business

Woodmancote School
Station Road
Woodmancote
Cheltenham
Gloucestershire
GL52 9HN

T – 01242 674312
W – www.woodmancote.gloucs.sch.uk

Woodmancote School
Belong · Aspire · Achieve

Appendix 6

Flow chart for Managing an E-Safety Incident

Following an incident, the eSafety coordinator or Headteacher will need to decide quickly how it should be dealt with.

Unsuitable material/illegal material/unsuitable activity/illegal activity is found or suspected on school's network of resources

↓

Identify those involved, if known, without compromising any potential evidence (staff, child, visitor or unknown, and decide whether they are a victim or instigator)

↓

Isolate any equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out

↓

Report to Designated Safeguarding Lead (DSL) and/or if appropriate to the local e-Safety coordinator

↓

Is there a child protection concern?

Yes ↓

No →

Is it an adult safeguarding concern?

Yes ↓

No →

Seek advice or make a request for Service through the Childrens Helpdesk (Tel: 01452 426565)
Or Report as appropriate toLADO (Tel: 01452 426994)

↓

Is illegal or unsuitable material or activity found or suspected?

Yes ↓

Examples of illegal activity:
Downloading pornography
Passing onto others images or videos containing child pornography
Inciting racial or religious hatred
Promoting illegal acts

Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to DBS

↓

Is illegal or unsuitable material or activity confirmed?

Yes ↓

Police or relevant organisation take action

No →

No ↓

Review incident, agree and implement appropriate actons. Suggested possible actions include:

- Inform parents/guardians
- Review or create risk assessment
- Counselling
- Referral to other agency
- Disciplinary procedures

↓

Debrief all relevant parties at end of e-safety incident

↓

Review all policies and procedures

↓

Organise knowledge share session

If you believe a child is at risk or in immediate danger you should do one of the following:

- Follow schools Safeguarding reporting procedures
- Call the Police on 999
- Or make a referral to the Social Care desk
- Immediately isolate the equipment to avoid

Woodmancote School
Belong · Aspire · Achieve

Appendix 5 – model loan contract

Woodmancote School
Belong · Aspire · Achieve

Appendix 7

Woodmancote School eSafety Incident Log

Details of ALL e Safety incidents to be recorded by the eSafety co-ordinator. This incident log will be monitored by the Headteacher.

Date & Time	Name of pupil or staff	Male Or Female	Computer or Class	Details of incident (including evidence)	Actions and Reasons

Woodmancote School
Belong · Aspire · Achieve

Appendix 8

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to eSafety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence

liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another persons password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.