E-Safety and Data Security Policy

Document History and Version Control Summary	
Version Number	1.0
Last Amendment	November 2014
Reviewed by	Learning and Achievement Committee
Date Revised	November 2014
Review Date	November 2015

WGS E-Safety and Data Security Policy

Document Control Information	Notes
• Document Title	WGS E-Safety and Data Security Policy
• Document Author	RY
• Version Number	1.0
• Date policy adopted by SLT/Governors	November 2013
• Frequency of Review	Annual
• Date Next Review Due	November 2014
Consultation Checklist: stakeholders views/approval from	
• Student Council Y/N	N
• Parents and Carers Y/N	N
• Staff (please list initials or staff groups e.g. HoDs)	For v 0.1 and 0.2: RWS, AS, NAV, IDT; DJA For v 0.3: SLT; For v0.4: Staff; For V0.5 SLT
• SLT (for approval)	v 0.5
• Governors (for adoption)	V 0.6
• Other (please enter details)	
Publication and Dissemination Checklist	
• Document Published to WGS Intranet (Woody)	N
• Document Published to External Website Y/N	Y
• Document version updated on internal shared drive Y/N	Y
• Document version updated on external website Y/N	Y
• Other WGS document referencing this policy edited Y/N	Y
• Relevant stakeholders informed of new version via email? Y/N	Y

Contents

Overview

The Wood Green School (WGS) *E-Safety and Data Security Policy* sets a programme of action to protect a) school users of ICT and associated technologies and resources (e-safety) and b) the safety of information (data security) held at Wood Green School.

E-Safety Policy

This *E-Safety Policy* sets out internal processes and procedures to protect WGS students, staff and visitors making use of ICT and associated technologies and resources.

Both the *E-Safety Policy* and associated *Acceptable Use Policy* (AUP) and *AUP Agreement* are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

E-Safety in the Curriculum

We understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

- The school has a framework for teaching E-Safety skills as part of the ICT curriculum
- The school provides opportunities within a range of curriculum areas to teach about E-Safety

- Educating students about the online risks that they may encounter outside school is done formally as part of the E-Safety curriculum and, ad hoc, when opportunities arise
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them
- Students etc are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities and as part of the E-Safety curriculum
- Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

Email

The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and good network etiquette: 'netiquette'.

Managing email

- Students have their own individual school issued accounts. Students are introduced to email and associated E-Safety issues as part of the ICT Scheme of Work
- The school gives all staff their own email account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is monitored by sampling.
- The school email account must be the account that is used for all school business
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses
- 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
- All emails should self-checked carefully for accuracy, spelling and grammar before sending
- Staff sending emails to external organisations, parents or students are advised to cc their line manager or designated account
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:
    - Delete all emails of short-term value
    - Organise email into folders and carry out frequent house-keeping on all folders and archives
- The forwarding of chain letters is not permitted in school. However the school has set up a concerns@woodgreen.oxon.sch.uk to allow students to forward any chain letters causing them anxiety. No action will be taken with this account by any member of the school community
- All student email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments

- Students must immediately tell a teacher/ trusted adult if they receive an offensive email
- Staff must inform the E-Safety co-ordinator or their line manager if they receive an offensive email
- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply

Sending emails

- Use your own school email account so that you are clearly identified as the originator of a message
- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary for effective communication
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School email is not to be used for personal advertising
- Where your conclusion is that email must be used to transmit personal, sensitive, confidential or classified information:
  - Obtain express consent from your manager to provide the information by email
  - Exercise caution when sending the email and always follow these checks before releasing the email:
  - Encrypt and password protect data. See http://www.thegrid.org.uk/info/dataprotection/#securedata for advice
  - Verify the details, including accurate email address, of any intended recipient of the information
  - Verify (by phoning) the details of a requestor before responding to email requests for information
  - Do not copy or forward the email to any more recipients than is absolutely necessary
  - Do not send the information to anybody/person whose details you have been unable to separately verify (usually by phone)
  - Send the information as an encrypted document attached to an email
  - Provide the encryption key or password by a separate contact with the recipient(s)
  - Do not identify such information in the subject line of any email
  - Request confirmation of safe receipt

Receiving emails

- Check your email regularly and at least three times a week
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; Consult your Network Coordinator first
- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of emails is not allowed

Internet Access

Managing the Internet

- The school provides students with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity
- Staff will preview any recommended sites before use
- Raw image searches are discouraged when working with students
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this 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

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience
- Do not reveal names of colleagues, students, others or any other confidential information acquired through your job on any social networking site or other online application
- On-line gambling or gaming is not allowed
- It is at the Headteacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

IT Infrastructure

- School internet access is controlled through a web filtering service which is the responsibility of the Network Coordinator
- Wood Green 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
- Staff and students are aware that school based email and internet activity can be monitored and explored further if required
- The school does not allow students access to internet logs
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate
- It is the responsibility of the school, by delegation to the Network Coordinator, to ensure that anti-virus protection is installed and kept up-to-date on all school machines
- Students 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 nor the Network Coordinator's to install or maintain virus protection on personal systems.
- Students and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Network Coordinator
- If there are any issues related to viruses or anti-virus software, the Network Coordinator should be informed by email

Social Networking

- At present, the school endeavours to deny access to social networking and online games websites to students within school
- All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online
- WGS students are asked to report any incidents of Cyberbullying to the E-Safety Officer
- Staff may only create blogs, wikis or other online areas in order to communicate with students using the school learning platform or other systems approved by the Headteacher

Twitter

- The official Wood Green School Twitter feed, @WGSWitney, aims to provide information about school news, events and success for students, parents and the wider community.
- Only nominated staff are authorised to publish messages on the @WGSWitney ie tweet and are responsible for the content of messages.
- Students are encouraged to submit tweets for publication by emailing tweets@woodgreenschool.oxon.uk. Student tweets are checked and then published on @WGSWitney by an authorised member of staff
- The school does not follow other Twitter users but may retweet relevant messages by others eg the Department for Education
- @WGSWitney encourages student, staff, parent and community followers. Advice on safeguarding the online identity of students is part of the e-safety curriculum
- All @WGSWitney messages are read and passed on to the appropriate party in the school but no reply is sent via Twitter to the sender. Individuals and organisations are asked to use email for correspondence requiring a reply.

- The school welcomes appropriate referencing and mentioning of its Twitter feeds.
- Individuals posting offensive remarks aimed at the school, its students, staff, parent, governors will have their follow status barred and, depending on the nature of the comment, may be reported to the relevant authority
- The school provides departments with dedicated Twitter accounts to use solely for educational purposes e.g. @WGSEconomics. The main purpose of departmental Twitter accounts is to enable the sharing of resources for a given course e.g. A Level Economics. Only staff may post tweets on departmental Twitter feeds.
- Staff are not permitted to direct message students using Twitter. Official school email accounts should be used for correspondence about teaching and learning that requires a reply.

Safe Use of images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember 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 students) and staff, the school permits the appropriate taking of images by staff and students with school equipment

Staff are permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips provided images taken are transferred immediately and solely to the school's network and deleted from the staff device

Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff and others without advance permission from the Headteacher.

Students and staff must have permission from an authorised member of staff before any image can be uploaded for publication

Consent of Adults Who Work at the School

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

Consent of students

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school website
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- on the school's learning platform or Virtual Learning Environment
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form 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, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. Email and postal addresses of students will not be published. Students' full names will not be published.

Before posting student work on the internet, a check needs to be made on SIMs to ensure that permission has been given for work to be displayed.

- Only authorised staff may upload content to the school site.

For further information relating to issues associated with school websites and the safe use of images see best practice as set out for Hertfordshire schools:

- http://www.thegrid.org.uk/schoolweb/safety/index.shtml
- http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

Storage of Images

- Images/ films of children are stored on the school's network and archives
- Students and staff are not permitted to use personal portable media for storage of such 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 students within the confines of the school network or other online school resource
- Network Coordinator or designated ICT Technician has the responsibility of deleting the images when they are no longer required

Webcams and CCTV

- The school uses CCTV for security and safety. Only staff nominated by the Headteacher can access CCTV video. Notification of CCTV use is displayed at the front of the school.
- We do not use publicly accessible webcams in school
- Webcams in school are only ever used as CCTV for security and safety or for specific learning purposes, e.g. monitoring hens' eggs and never using images of children or adults
- Misuse of the webcam by any member of the school community will result in sanctions
- The school does not currently have any webcams. If introduced areas with webcams will be indicated by signage.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school
- All students are supervised by a member of staff when video conferencing
- All students are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences
- No part of any video conference is recorded in any medium without the written consent of those taking part

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be CRB checked
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

Computer Viruses

- All files downloaded from the internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used
- Never interfere with any anti-virus software installed on school ICT equipment that you use
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact IT Support immediately.

Data Security Policy

Data Security Overview

This WGS Data Security Policy sets out internal WGS process for to protect online privacy, to minimise risks to data security, and to comply with the law.

WGS complies with The Data Protection Act (1988) for example, only essential information is collected, that it is secure and held only as long as is necessary.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Classification of Data

The accessing and appropriate use of school data is something that the school takes very seriously. Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Wood Green uses three categories to classify information assets:

- **Restricted**: Personal information related to students or staff
- **Protected**: General school information not expected to be released to the public
- **Public:** Information freely available to anyone

Confidential information about individuals is **restricted** and

- can only be accessed by named individuals or groups
- is generally stored in the WGS Management Information System
- if printed on paper is labelled confidential

Access Control: user access

- Access to all ICT systems shall be via unique login and password. Any exceptions shall be approved by the Senior Information Risk Officer (SIRO).
- Where possible, all information storage shall be restricted to only necessary users. Access granted to new groups of users (for example, an external group attending a school-based event) shall be approved by the SIRO.
- All requests for access beyond that normally allocated (e.g. teachers wishing to access student personal storage) shall be authorised by the SIRO. This shall include the authorisation of access required by the ICT Support Team during investigations.
- Where 'restricted' information is stored, access shall only be granted to individuals approved by the SIRO. A record shall be kept of these approvals.
- All access controls should be reviewed each term, to ensure that any users that leave have their access removed.

Access Control: The Network

Responsibility: Technical Support Staff

- Where any external network traffic is allowed from the internet to the school, a local firewall shall be deployed to restrict traffic to only necessary ports and IP addresses.
- Where the school's external internet connection allows connections from other schools behind a shared firewall, a local firewall should be considered to restrict this traffic.
- All internet-facing systems shall be placed onto a separate network segment; a de-militarised zone (DMZ), with access to applicable services, controlled by a firewall.
- Where externally facing services may be at particular risk, the addition of an Intrusion Prevention System (IPS) should be considered.
- The use of external specialist third-party penetration testing should be considered on an annual basis for internet visible systems.
- All wireless implementations shall be a minimum of WPA 2 encryption, and shall require authentication prior to connection. Where possible, wireless networks should be further restricted through the firewall.
- The use of shared folders on workstations and laptops should be discouraged. If used ensure folders are password protected.

Password Security

Passwords are an important aspect of information security, and are the usual way to protect access to information. As such, all members of staff with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords. These steps should include:

- Keeping their password secure from students, family members, and other staff.
- Using a different password for accessing school systems to that used for personal (non-school) purposes.
- Choosing a password that is difficult to guess, or difficult for students to obtain by watching staff login.
- Adding numbers or special characters (e.g. !@£$%^) can help.
- Changing passwords regularly
- Staff should try not to write down their password, unless absolutely necessary and then in a location that cannot be accessed by anyone else.
- In addition, when leaving a computer for any length of time, all staff shall log off or lock the computer, using CTRL+ATL+DELETE.
- Ensuring that there is a limit on the number of consecutive failed log in attempts
- Access credentials (passwords) should not be stored within the machines internet browser or any remote access software.

Starters and Leavers

- The IT Support Team must be informed promptly of any student or member of staff joining or leaving the school: NM or ICT team receive email from either 11-16 or 6th Form admin staff advising of in-term moves and those remaining for 6th Form after GCSE results

- Any school owned ICT equipment should be returned to the IT Support Team when staff leave.
- The IT Support Team shall ensure that leavers' access is removed, or disabled, in a timely manner.

Protecting Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- Only download personal data from systems if expressly authorised to do so by your manager
- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling e.g. restricted documents must be shredded

Storing/Transferring Information Using Removable Media

- Always consider if an alternative solution already exists e.g. WGS SkyDrives
- Store all removable media securely
- Encrypt all files containing personal, sensitive, confidential or classified data
- Removable media must be disposed of securely by your ICT support team

Remote Access

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone
- Select PINs to ensure that they are not easily guessed, e.g. do not use your house or telephone number or choose consecutive or repeated numbers
- Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is

- Protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity
- Ensure that all ICT equipment that you use is kept physically secure
- Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990
- It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable device. If it is necessary to do so the local drive must be encrypted
- A time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles
- To ensure security, privately owned ICT equipment should not be used on a school network without the permission of the Network Coordinator
- On termination of employment, resignation or transfer, return all ICT equipment to the Network Coordinator. You must also provide details of all your system logons so that they can be disabled
- It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person
- All ICT equipment allocated to staff must be authorised by Director of Digital Learning
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey
- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- The installation of any applications or software packages must be authorised by the Network Coordinator, fully licensed and only carried out by your ICT support

- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight
- Portable equipment must be transported in its protective case if supplied

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device
- Students are not allowed to bring phones into school
- Other personal mobile devices e.g. graphic tablets may be used for educational purposes,
- 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
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and that their power supply has been recently PAT tested.

Disposal of Redundant ICT Equipment Policy

All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any ICT equipment will conform to:

- The Waste Electrical and Electronic Equipment Regulations 2006
- The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007
- Data Protection Act 1998
- Electricity at Work Regulations 1989

WGS maintains a comprehensive inventory of all its ICT equipment including a record of disposal. If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

Monitoring

Monitoring Procedures

Authorised IT Support staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using school ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Incident Reporting

All staff and students have a responsibility to report E-Safety or data security incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact on the school

Common incidents include

- Circumventing the network security system
- Accessing inappropriate material i.e. material that is obscene, offensive, illegal or inaccurate or likely to make the recipient feel threatened or worried
- Installing unapproved software
- Using other people's email addresses or passwords
- Breaching copyright
- uploading school material onto a social network or chat room
- Leaving school mobile devices unattended
- Not logging off when leaving a device

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to a) the school's SIRO or E-Safety Co-ordinator and b) Network Coordinator.

Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner, and Network Coordinator.

E-Safety and Data Security breaches are recorded in an Incident Log held by SIRO.

E-Safety and Data Security breaches Incident Log					
Incident Date:	What happened	Action Taken re this incident t	Actions to prevent reoccurrence	Legal implications	Closed date

The Incident Log is formally reviewed once per term by the SLT

Breaches

A breach or suspected breach of *E-Safety and Data Security Policy* by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, the LA Disciplinary Procedure or Probationary Service Policy.

Policy breaches may also lead to criminal or civil proceedings.

Dissemination

A copy of the *WGS E-Safety and Data Security* can be found on the school website

To help ensure on-going compliance,

- Staff AUPs are revisited at the beginning of each academic year at the first staff meeting
- The first lessons in ICT revisits student AUPs

- The potential risks and rewards of social networking forms part of the Enrichment Programme in both years 8 and 9.

WGS ICT Acceptable Use Agreement: Students

- I will use ICT systems in school, including the internet, email, digital video, and mobile technologies only for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own user name and password.
- I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students and/ or staff will only be taken with the permission of those involved and stored and used for school purposes in line with school policy. Images will not be distributed outside the school network without the permission of the Senior Information Risk Officer.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

✂_____ (please return)

Dear Parent/ Carer

ICT including the internet, email, mobile technologies and online resources have become an important part of learning in our school. We expect all students to be safe and responsible when using any ICT. It is essential that students are aware of E-Safety and know how to stay safe when using any ICT. A copy of the *WGS E-Safety and Data Security* can be found on the school web site

Students are expected to read and discuss this agreement with their parent or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or E-Safety coordinator.

We have discussed this document and ..... (student name) agrees to follow the E-Safety rules and to support the safe and responsible use of ICT at the School.

Parent/ Carer Signature .....

Student Signature.....

Form ..... Date .....

Copyright Release and Images Permission Form

Copyright Release for Student's Work

Wood Green School may produce web pages, ICT presentations, educational or interest articles for magazines or similar including materials created by students. No child's work will ever be used without their permission but we also need permission from the parents to be able to publish the student's work. Please rest assured the child's safety will always be of paramount importance and no personal information will be made public.

Acceptable Use of Images of Children

To comply with the Data Protection Act 1998, we need your permission before we can photograph or make any video recordings of your child for promotional purposes. For example, in the school prospectus and other printed publications that we produce for promotional purposes; project display boards around the school; on our website

Conditions of use

1. This form is valid for five years from the date you sign it, or for the period of time your child attends this school. The consent will automatically expire after this time.
2. We will not re-use any photographs or recordings after your child leaves this school
3. We will not use the personal details or full names (which means first name and surname) of any child or adult in a photographic image on video, on our website, in our school prospectus or in any of our other printed publications without good reason. For example, we may include the full name of a student in a newsletter to parents if the student has won an award.
4. If we name a student in the text, we will not use a photograph of that child to accompany the article without good reason.
5. We will not include personal email or postal addresses, or telephone or fax numbers on video, on our website, in our school prospectus or in other printed publications.
6. We may include pictures of students and teachers that have been drawn by the students.
7. We may use group or class photographs or footage with very general labels, such as "a science lesson" or "making Christmas decorations".
8. We will only use images of students who are suitably dressed, to reduce the risk of such images being used inappropriately.

Copyright Release and Images Permission

I consent for the school to publish my child's work on the internet subject to strict confidentiality of personal information.

I have read the school policy and give consent for the publication of images in which my child appears subject to the conditions of the policy.

Parent/ Carer Signature _____ Date _____

Name of Student _____ Form _____

A copy of the *WGS E-Safety and Data Security* can be found on the school web site

WGS ICT Acceptable Use Agreement: Staff

ICT (including data) 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 Senior Information Risk Owner or E-Safety Coordinator.

- I will use the school's email / internet / intranet / learning platform and any related technologies only for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT 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 students 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 students.
- I will use only the approved, secure email system(s) for any school business.
- I will ensure that personal and restricted data (such as data held on MIS software) 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. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware of software without permission of the Network Coordinator
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- 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 and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature ..... Date .....

Name .....(printed)

Job title .....

A copy of the *WGS E-Safety and Data Security* can be found on the school web site

Roles and Responsibilities

Governors

Governors are responsible for the approval of the *E-Safety and Data Security* Policy and for reviewing the effectiveness of the policy

Headteacher

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator

E-Safety Coordinator:

The responsibility for e-Safety are as follows:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with school IT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly at Senior Leadership Team meetings to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of Governors

Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) has the following responsibilities, they:

- own the information risk policy and risk assessment
- work with the Data Controller to determine the purposes for which and the manner in which any personal data are, or are to be, processed
- keep a record of all Information Asset Owners (IAOs)
- act as an advocate for information risk management

Data Controller

The WGS Data Controller works with the Senior Information Risk Officer to determine the purposes for which and the manner in which any personal data are, or are to be, processed

The responsibility of the data controller is to

- respond to access requests for information held by the school
- ensure personal data is only kept for as long as necessary
- ensure any sharing of WGS data with other organisations or individuals itself complies with the data protection principles
- it is lawful for the receiving organisation or body to receive and use the personal data;

Information Asset Owner (IAO)

The role of an IAO is to understand:

- what information is held, and for what purposes
- what information needs to be protected and how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed off

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements.

Network Coordinator

The Network Coordinator is responsible for ensuring that

- the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the WGS Acceptable Usage Policy and any relevant WGS Policies and guidance
- that users may only access the school's networks through a properly enforced password protection policy
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator
- that monitoring software / systems are implemented and updated as agreed in school policies

Head of ICT

The Head of ICT is responsible for ensuring that a comprehensive and developmental e-safety curriculum for students referenced in ICT schemes of work and programmes of study. The programme includes the responsible use of web and communication technologies both inside and outside school and risks related to cyber-bullying.

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable IT Use Policy and Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction

- digital communications with students / students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school e-safety and acceptable use policy
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extracurricular and extended school activities
- are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection Officer

The Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:

- are responsible for using the school ICT systems in accordance with the Student Acceptable IT Use Policy. They will be expected to sign an Acceptable Use Agreement before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters,

website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Agreement
- accessing the school website / VLE / on-line student / student records in accordance with the relevant school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems / website / VLE as part of the Extended School provision will be expected to sign a Staff User AUP Agreement, before being provided with access to school systems

Sources

The WGS *Acceptable Use Policy for E-Safety and Data Security* is developed from national guidance and LEA best practice. In particular:

- Hertfordshire LEA model E-Safety and Data Security Guidance Policies for ICT Acceptable Use (26/03/2012)
- Kent LEA School E-Safety Schools Policy
- Staffordshire LEA e-safety toolkit
- National Education Network: E-Safeguarding: Creating Working Procedures in Schools.
- DfE: Principles of e-safety: Acceptable Use Policies (AUPs)

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) and (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 E-Safety

Racial and Religious Hatred Act 2006

It is 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 see www.teachernet.gov.uk

Equality Act 2010

The Equality Act simplifies, strengthens and harmonises current legislation to provide a new discrimination law which protects individuals from unfair treatment and promotes a fair and more equal society. The equality duty came into force in April 2011 and covers the following Personal Protected Characteristics :1. Age 2. Disability 3. Gender (male/female) 4. Gender reassignment 5. Marriage and civil partnership* 6. Pregnancy and maternity 7. Race 8. Religion or belief 9. Sexual orientation

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 (email) 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.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx