1. **What is E-Safety**

As a learning community, Washwood Heath Academy wants all staff and students to be able to be safe users of ICT and all data storage. The development of responsible, independent users is a prime aim of our Academy in developing people and helping them to be safe, happy and successful.

E-safety stands for electronic safety: being safe when using all electronic devices.

Embedded in every teacher’s terms and conditions is the “duty to care” and this requires teachers to take steps to ensure that the children in their care are safe and secure and this applies as much to e-safety.

The aim of our school is to ensure both staff and students are aware of e-safety and the threats to it, by developing the skills and knowledge of all in the school community so that they can use digital technology and the Internet responsibly and safely.

However e-safety is not just the remit of the ICT teacher/ ICT Coordinator/ Head of Department but also every teacher whenever and wherever they make use of ICT with students.

ICT resources are a powerful and positive learning tool, but there are risks involved. Left unnoticed and unchecked, computer misuse can have serious consequences.

Washwood Heath School works in four areas to protect our students while on-line:

- **Educating Staff**
  - All Staff are given Children Protection and e-Safety training when they arrive at school and at the start of each school year.
  - All Staff sign a Staff Acceptable Use Policy.
• Educating Students
  • Students receive e-Safety lessons within ICT Lessons and have a “Keep Safe Day” which features e-safety.

  • In Year 7 the first unit students do is E-safety. Topics covered are:
    • Login Procedure
    • Passwords and usernames
    • School’s computer use policy
    • Monitoring software – AB Tutor
    • Mobile Technology
    • Cyber-bullying
    • Internet and Email
    • Phishing
    • Where to report abuse (thinkuknow – website)
    • What to do in different scenarios (homework)
    • Awareness of sanctions and removal of privileges

• Students sign an Acceptable Use Policy every time they access school computers. This states the following:

  **Responsible Computer and Internet Usage:**
  • I will use the school computers and internet access for learning.
  • I understand the school computers are a valuable resource for my education; I will not abuse this facility by playing games during lessons.
  • I will only use my own login and password.
  • I will not damage the academies ICT equipment.
  • I will not look at or delete other people’s files.
  • I will only save files that I use in my schoolwork to the school network.
  • I know the school can check my computer files and may monitor the Internet Sites I visit.
  • I understand that if I deliberately break these rules, the school will discipline me.
• The school has the following tools to protect students:

  • Webwasher
    BGfL use Webwasher filtering for all schools to restrict content, once a site has been classified as undesirable students and staff cannot gain access.

  • AB Tutor
    All computer suites have AB Tutor, which allows teachers to take control of the classrooms by stopping Internet Access or allowing software which is not normally accessible.

    All staff members are able to restrict students by applying or removing rules like:
    - Block Internet Access
    - Block Printing
    - Moodle Only
    - Office Programs Only

• Tools to monitor website access
  • Policy Central Enterprise
    Policy Central compliments these tools as it can block website, but can be applied it across all school systems
    Policy Central is responsible for the Acceptable Use Policy that each student agrees on logging into an school computer.
    A log of websites is taken and monthly reports are analysed to review student behaviour online.

2. Using the Internet in Lessons

Evaluating and reviewing online resources
It is important to determine the reliability and accuracy of the material is found on the internet. Teachers should critically evaluate websites when selecting resources for use in the classroom, and students should also be taught these skills as part of their digital literacy skills development.
Images

Staff must take care with the images they and their students have on their screens and report any concerns to the Associate Head Teacher (Curriculum/Evaluation) and the ICT Operations Manager.

3. E-Safety Incidents
   • Any E-Safety Incidents should be reported to the Associate Head Teacher (Curriculum/Evaluation), unless it is a child protection issue in which case, the relevant procedures are followed.
   • Any issues related to staff will be passed to the Executive Head Teacher in first instance.
   • A disclosure log is maintained of all e-safety issues, which is held by the ICT Operations Manager.

4. Cyber-bullying
   • Staff will receive training in identifying cyber-bullying and understanding their responsibilities. The DSP will liaise with the Network Manager on this matter.
   • All staff will be helped to keep up to date with the technologies that children are using.
   • Students will be educated about cyber-bullying through a variety of means:
     - ICT Curriculum
     - Keep Safe/Anti-Bullying programmes for all years in Dimension Days
     - Anti-bullying Week Assemblies.

5. Passwords
   It is staff member’s responsibility to keep their password a secret, to change it if they suspect that there is a risk of anyone else knowing it, which they must report to both the Associate Head Teacher (Curriculum/Evaluation) and the ICT Operations Manager.
Note:
If a student should gain access to a staff member’s account, under the Data Protection Act (1998), the staff member are at fault for allowing them access.

6. School Supplied Laptops

On beginning to work at the school, the IT Technicians will issue all teaching and classroom based staff with a laptop.
- Staff are responsible for taking a back-up of their school data from their laptop to your Home Folder on the school network.
- Laptops are supplied encrypted with Truecrypt, an open source encryption software system.
- All USBs and external Hard Drives that hold student and staff data must be encrypted with Truecrypt. All staff agree to do this in the Acceptable Usage Policy.

7. Mapped Network Drives

Staff should only save school information to the school network.

8. WHoodle

- The school uses Moodle as its VLE.
- The school has a secure Teacher area called “Staff Room”, which hold information to be shared with the staff.
- This information can be accessed remotely.
- Staff must not share this password with anyone or auto-save it on your web browser.

9. Student Hand-In Folders

- Within Project Folders each Teacher will have a hand-in folder. This allows students to drag and drop their work into this network space for assessment.
- Students are not able to directly save the work from inside programs like MS Word.
• Students are not able to remove their work from this folder or read other students’ work.

10. Student Email
• The school issues each student with a Zimbra email account which takes the form: 12a12345@whtc.bham.org.uk
  Emails sent from these accounts are moderated and foul and abusive language is sent to the Zimbra Administrator.

11. Staff Email
• The school issues staff with an email account based on their staff code in ePortal. It will take the form: abc@washwoodheath.bham.sch.uk
• Staff have web access to email; this can be accessed from www.washwoodheath.com.
• Staff should always use the school email when carrying out school business and check email regularly each day through the day.
• If emailing parents, staff should use the ‘enquiry’ email account. To make use of this service staff should send the details to the Administration Team, who will send the email.
• If staff require the school to keep a copy of any emails that are of a sensitive nature, they send a blind copy to archive@washwoodheath.bham.sch.uk. This can only email to the archive address from a school email account.
• Staff must not let students know their private email account.
• Staff should not send school related emails using their private email account.
• Staff should not use their school email address to sign up for offers.
• Personal Message Manager (PMM) is in place to filter spam and unwanted emails, but legitimate emails will get caught by this system. When staff release a legitimate email they will be asked if the address should be added to their safe senders list.
12. **EPortal**
   - The school uses CMIS as its management system, which has ePortal as its Teachers Management Tool.
   - All teachers are issued with an ePortal account for registration and student reports.
   - Staff must not share this password with anyone or auto-save it on their web browser.

13. **Mobile phones**

   Staff should take care when using personal mobile phones.

   - Personal mobile number should not be used to communicate with students or parents.
   - If unavoidable, number should be withheld by entering 141 before dialling or change your mobile phone settings so caller ID is not shown.
   - Texts to parents must only be sent using the school’s ‘Keep Kids Safe’ text service.
   - Staff must not:
     - take photos of students using a mobile phone
     - use a mobile during lessons unless an emergency.
     - lend a mobile phone to students

   Staff should also refer to the ‘Use of own devices policy’.

14. **Personal Internet Usage**

   - There should be no personal use of the internet during student contact time.
   - Visiting offensive websites using the school facilities is prohibited.
   - If staff accidentally access inappropriate material, please inform the ICT Operation Manager and SLT so internet filters can be updated.

   Staff must not comment about students, colleagues, the community, the School or its partners in their personal internet use or make comments which could be viewed.
15. Photography and Video
- Ensure parental preference is followed regarding photography and video.
- Staff must be able to justify any images/videos of students in their possession.
- ICT equipment (including photography and video resources) belonging to the school should only be used for work purposes.
- Personal photography/video equipment should not be used to record school activities. If unavoidable, images should be transferred to school ICT equipment immediately.

16. Social Networking
- Staff should not become online ‘friends’ with students and think carefully about ‘friending’ parents or previous students.
- It is not acceptable for staff to make inappropriate comments about their workplace or colleagues on any social media or blog facility.
- It is not acceptable for staff to use any social networking sites like Facebook, Bebo, Myspace, Flickr or Twitter, or to blog during working hours.
- It is not acceptable for staff or students to make inappropriate comments about the establishment staff or student body on a social network website, or place photographs of them on such sites without permission. Any incidents of this nature should be reported to the SLT.
- Staff are advised to frequently check their privacy settings on social networking sites to ensure they can control who can see the information shared about them, taking care regarding the type of information they publish about themselves or personal photographs.

17. E-Safety Committee
Washwood Heath Academy has implemented an e-safety committee to provide a consultative group that represents the school community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy. The committee will also include (not exclusively) the PSHEE Coordinator, an ICT Teacher, the ICT Operations Manager and a member of the Administration Team.

They take responsibility for updating this e-safety policy document and will hold termly meeting to discuss policy and new developments in e-safety.

18. **Acceptable Usage Policy (AUP) for Staff**
   - All staff members are asked to sign the Acceptable Usage Policy on joining the school, contained in the Data Protection Policy.
   - Once signed the form should be returned to the HR Manager