WALLINGTON HIGH SCHOOL FOR GIRLS

E-SAFETY POLICY

CONTENTS

Reference Documents:

1. Search and Confiscation guidance from DfE
   https://www.gov.uk/government/publications/searching-screening-and-confiscation
2. Behaviour for Learning Policy
3. Data Protection Policy

Appendices:

1. Acceptable Use Agreement (Staff and Students)
2. Bring Your Own Device Protocol

1. INTRODUCTION AND OVERVIEW

1.1 Rationale and Scope

1.1.1 Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Wallington High School for Girls with respect to the use of ICT-based technologies;
- safeguard and protect the children and staff of the school;
- assist school staff to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice;
- set clear expectations of behaviour and / or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use;
- have clear structures to deal with online abuse such as cyberbullying;
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content:

- exposure to inappropriate on-line content
- content validation: how to check the authenticity and accuracy of online content

Contact:

- grooming
- cyber-bullying
- identity theft and sharing of passwords

Conduct:

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being
- sexting

1.1.2 Scope of the Policy

This policy applies to all members of our community who have access to and are users of our ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

1.2 Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision. • To take overall responsibility for data and data security as Senior Information Risk Owner (SIRO). • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive regular monitoring reports from the Designated Person for Child Protection. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures (e.g. network manager).
Designated Person for Child Protection / E-safety Co-ordinator	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documentation. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-safety education is embedded across the curriculum. • Liaises with school ICT technical staff. • Communicates regularly with SLT and the designated e-safety Governor to discuss current issues and review incident logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • To ensure that e-safety incidents are recorded according to safeguarding record-keeping procedures as appropriate. • Facilitates training and advice for all staff. • Liaises with the Local Authority and relevant agencies. • Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues to arise from e-safety matters.
Governors / E-safety Governor	• To ensure that the school follows all current e-safety advice to keep the students and staff safe. • To approve the e-safety Policy and review the effectiveness of the policy. This will be carried out by the Governors Curriculum Committee. A member of the Governing Body has taken on the role of e-safety Governor (Sandy Gillett). • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the E-Safety Governor will include an annual review with the E-Safety Co-ordinator.
Computer Science Curriculum Leader	• To oversee the delivery of the e-safety element of the Computer Science curriculum. • To liaise with the E-safety Co-ordinator on e-safety matters as appropriate.

Role	Key Responsibilities
Network Manager / ICT Technician	• To report any e-safety related issues that arise to the Designated Person for Child Protection. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date). • To ensure the security of the school ICT system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • **T**he school's policy on web-filtering is applied and updated on a regular basis. • That they keep up-to-date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of the network / Managed Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the designated person for investigation. • Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • Keep up-to-date documentation of the school's e-security and technical procedures. • Ensure that all data held on students on the school office machines have appropriate access controls in place.
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities. • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular activities if relevant). • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's e-safety policies and guidance. • To read, understand and adhere to the school staff Acceptable Use Agreement (Appendix 1) and Bring Your Own Device (BYOD) protocol (Appendix 2). • To be 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. • To report any suspected misuse or problem to the Designated Person. • To maintain an awareness of current e-safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own use of technology. • To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc..

Role	Key Responsibilities
Students	• Read, understand and adhere to the Student Acceptable Use Policy and BYOD protocol. • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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. • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • To help the school in the creation / review of e-safety policies.
Parents / carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the Internet and the school's use of photographic and video images. • To read, understand and promote the school Student Acceptable Use Agreement and BYOD protocol with their children. • To access the school website / MLE / on-line student records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology.
External groups	• Any external individual / organisation will read an Acceptable Use Policy prior to consent being given passwords to use any equipment or the Internet within school.

1.3 Communication:

The policy will be communicated to staff, students and Governors in the following ways:

- Policy to be posted on the school website with edited parts in the student planner.
- Policy to be part of the school induction pack for new staff and a signed acknowledgement to be completed once read.
- Acceptable use agreements discussed with students at the start of each year as part of tutor time when planners are allocated.
- Acceptable use agreements to be issued to new students on entry to the school.

1.4 Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the

Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview / counselling by tutor / Head of Year / Designated Person / Headteacher;
  - Informing parents or carers;
  - Removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - Referral to Local Authority / Police.
- Our Designated Person acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / Local Authority child protection procedures.

1.5 Review and Monitoring

The e-safety policy should be read in conjunction with the following policies; Child Protection Policy, Data Protection Policy and Behaviour for Learning Policy. The school has an E-safety Co-ordinator (Designated Person for Child Protection) who will be responsible for document ownership, review and updates.

- The E-safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The E-safety Policy has been written by the designated person and is current and appropriate for its intended audience and purpose.
- The policy and has been agreed by the SLT and approved by Governors.

2. EDUCATION AND CURRICULUM

2.1 Pupil E-safety Curriculum

This school:

- has a clear e-safety education programme as part of the Computer Science curriculum / PSHCE curriculum / Assembly programme / enrichment programme / tutor time programme. It is built on best practice in e-safety and covers a range of skills and behaviours appropriate to our students including:
  - to STOP and THINK before they CLICK;
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
  - to know how to narrow down or refine a search;
  - to understand how search engines work and to understand that this affects the results they see at the top of the listings;
  - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;

- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- to understand why and how some people will 'groom' young people for sexual reasons;
- to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying;
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through an Acceptable Use Policy which every student agrees to when using school based ICT networks;
- ensures staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include: risks in pop-ups; buying on-line; on-line gaming / gambling.

2.2 Staff and Governor Training

This school:

- ensures staff know how to send or receive sensitive and personal data;
- makes training and education on e-safety issues available to staff;
- provides, as part of the induction process, all new staff with information and guidance on the e-safety policy and the school's Acceptable Use Policy and BYOD protocol.

2.3 Parent awareness and training

This school:

- runs a rolling programme of advice, guidance and training for parents, including:
  - information leaflets, in the Wallington Week and on the school web site;
  - annual e-safety information evenings for parents held at school;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

3. EXPECTED CONDUCT AND INCIDENT MANAGEMENT

3.1 Expected conduct

In this school:

All users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they agree to before being given access to school systems;
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- 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;
- will be expected to know and understand school guidance 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.

Staff:

- are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Students / Students:

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents / Carers:

- should provide consent for students to use the Internet, as well as other technologies, at the time of their child's entry to the school;
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

3.1 Incident Management

In this school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (e.g. the local authority, CEOP, UK Safer Internet Centre helpline) in dealing with e-safety issues;
- monitoring, recording and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school;
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible;

- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law.

4. MANAGING THE ICT INFRASTRUCTURE

4.1 Internet access, security (virus protection) and filtering

This school:

- has the educational filtered secure broadband connectivity through Schools Broadband;
- uses a Smoothwall filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged;
- ensures network health through use of Sophos anti-virus software;
- has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network;
- is vigilant in its supervision of students' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older students have more flexible access;
- ensures all staff and students accept and agree to an Acceptable Use Policy and understands that they must report any concerns;
- ensures students only publish within an appropriately secure environment: the school's learning environment;
- requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; plans the curriculum context for Internet use to match students' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids, Google Safe Search.
- informs all users that Internet use is monitored;
- informs staff and students that they must report any failure of the filtering systems directly to the IT Support Team;
- makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through policy and CPD;
- provides advice and information on reporting offensive materials, abuse / bullying etc. available for students, staff and parents;
- immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

4.2 Network management (user access, backup)

This school:

- uses individual, audited log-ins for all users;
- uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;

- uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- ensures that storage of all data within the school will conform to the UK data protection requirements

To ensure the network is used safely, this school:

- ensures staff read the school's e-safety Policy;
- ensures staff access to the schools' management information system is controlled through the user's network account;
- provides students with an individual network log-in username;
- ensures all students have their own unique username and password which gives them access to the Internet, the MLE and email account;
- makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- has set-up the network with a shared work area for students and one for staff. Staff and students are shown how to save work and access work from these areas;
- requires all users to always log off when they have finished working or are leaving the computer unattended;
- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day. We automatically switch off all computers at 2100hrs to save energy;
- has blocked access to music / media download or shopping sites – except those approved for educational purposes;
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs;
- maintains equipment to ensure Health and Safety is followed;
- has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role; e.g. teachers access report writing module; SEN coordinator - SEN data;
- ensures that access to the school's network resources from remote locations by staff is restricted just as if they were logged onto the network locally;
- does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted, e.g. technical support or MIS Support, our Borough Attendance Service accessing attendance data on specific children, parents using a secure portal to access information on their child;
- provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their username and password;

- makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- uses the DfE secure s2s website for all CTF files sent to other schools;
- follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- ensures our wireless network has been secured to industry standard Enterprise security level / appropriate standards suitable for educational use;
- ensures all computer equipment is installed professionally and meets health and safety standards;
- ensures projectors are maintained so that the quality of presentation remains high;
- reviews the school ICT systems regularly with regard to health and safety and security.

4.3 Password policy

- This school makes it clear that staff and students must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

4.4 Email

This school:

- provides staff with an email account for their professional use;
- will contact the Police if one of our staff or students receives an email that we consider is particularly disturbing or breaks the law;
- will ensure that email accounts are maintained and up-to-date;
- reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;
- knows that spam, phishing and virus attachments can make emails dangerous. We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language.

Students:

- students are introduced to, and use email as part of the Computer Science scheme of work;
- students are taught about the safety and 'netiquette' of using email both in school and at home, i.e. they are taught:
  - not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent / carer;
  - that an email is a form of publishing where the message should be clear, short and concise;

- that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- they must not reveal private details of themselves or others in email, such as address, telephone number, etc.;
- to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
- that they should think carefully before sending any attachments;
- embedding adverts is not allowed;
- that they must immediately tell a teacher / responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature;
- not to respond to malicious or threatening messages;
- not to delete malicious of threatening emails, but to keep them as evidence of bullying.

Staff:

- access in school to external personal email accounts may be blocked;
- never use email to transfer staff or pupil personal data;
- staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
  - the sending of chain letters is not permitted;
  - embedding adverts is not allowed.

4.5 School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers.
- The school website complies with the statutory DfE guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website is the school address, telephone number and we use a general email contact address.
- Photographs published on the website do not have full names attached.
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website.
- We do not use embedded geodata in respect of stored images.
- We expect teachers using school approved blogs or wikis to password protect them and run from the school website.

4.6 Learning platform

- Uploading of information on the schools' MLE / virtual learning environment is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.

- Photographs and videos uploaded to the schools MLE will only be accessible by members of the school community.

- In school, students are only able to upload and publish within school approved and closed systems, such as the MLE.

4.7 Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- no reference should be made in social media to students / students, parents / carers or school staff;
- they do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions should not be attributed to the school or local authority;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

4.8 CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings, without permission except where disclosed to the Police as part of a criminal investigation.

5. DATA SECURITY

5.1 Management Information System Access

5.1.1 Strategic and operational practices

At this school:

- the Headteacher is the Senior Information Risk Officer (SIRO);
- there is a Data Protection Policy which outlines roles and responsibilities in regard to data security;
- all staff are DBS checked and records are held in the Single Central Record.

We ensure ALL the following school stakeholders must be authorised before using school systems and by using the system agree to our Acceptable Use Policy:

- governors,
- students,
- parents.

5.2 Data Transfer

5.2.1 This makes clear staff responsibilities with regard to data security, passwords and access.

- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and MLE access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

5.2.1 Technical Solutions

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer.
- Staff with access to the Admissions system also use separate user accounts.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- We lock any back-up tapes in a secure, fire-proof cabinet.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment, where any protected or restricted data has been held, and get a certificate of secure deletion for any server that once contained personal data.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using cross-cut shredder / collected by secure data disposal service.

6. EQUIPMENT AND DIGITAL CONTENT

6.1 Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, students & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Staff and students must adhere to the Bring Your Own Device protocol.
- The recording, taking and sharing of images, video and audio on any mobile phone is not permitted by the BYOD protocol. Such authorised use is to be closely monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.

- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

- Personal mobile phones will only be used during lessons with permission from the teacher.

- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

6.2 Digital images and video

In this school:

- we gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter joins the school;

- we do not identify students in online photographic materials or include the full names of students in the credits of any published school produced video materials / DVDs;

- if specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications, the school will obtain individual parental or pupil permission for its long term use;

- the school blocks / filters access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- students are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;

- students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;

- students are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

6.3 Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.

- Details of all school-owned software will be recorded in a software inventory.

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

- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen.

- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and / or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Date created: October 2015

Date to be reviewed: October 2016

Appendix 1

ACCEPTABLE USE STATEMENT (FOR STUDENTS AND STAFF) - April 2015 - WHSG IT Support

- The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Acceptable Use Policy has been drawn up to protect all parties - students, staff and the school. **By using the schools IT network and BYOD solution, staff and students agree to the Acceptable Use Statement.**

- The school reserves the right to examine or delete any files that may be held on its computer system and to monitor and log user activities on the Internet;

- Access must only be made via the authorised account and password, which must not be made available to any other person;

- All Internet use should be appropriate to staff professional activity or students' education;

- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden; e.g. introducing a virus;

- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed if they access these materials. Inappropriate materials should be reported to the IT Manager;

- Users are responsible for email they send and for contacts made that may result in inappropriate email being received - in line with LA guidance;

- The same professional levels of language and content should be applied as for letters or other media, particularly as email is often forwarded;

- Posting anonymous messages and forwarding chain letters is forbidden;

- Copyright of materials and intellectual property rights must be respected;

- Use of the Internet for personal financial gain, gambling, political purposes or advertising is forbidden;

- The school will not be held responsible for payment of any items ordered through the Internet, unless authorised by the Finance Department;

- Other users' files must not be accessed;

- Students at WHSG will not give their home address or phone number, or use the internet to arrange to meet anyone, unless their parent/carer or teacher has given them permission.

- The use floppy disks, CD-ROMs, memory sticks or any other form of removable is permitted. However, the user is responsible for checking said media for viruses before use.

- Staff must never use personal email accounts to contact students.

Appendix 2

'BRING YOUR OWN DEVICE'

BYOD Network Protocols

The principles from the school's Behaviour for Learning Policy, particularly the Anti-bullying Policy, apply to the use of the BYOD network.

Students should keep mobile devices and earphones in their blazer pockets or bags unless given permission in a teaching class, or they are in an area at a time when use of them is permitted.

Photography or filming is not allowed at any time without the express permission of a member of staff.

Devices must not be connected to any mobile data networks while on site (3G, 4G etc.), only filtered use of the BYOD network is authorised.

Phones should be kept on silent at all times.

Network Rules

- Whilst they are allowed to connect to the BYOD network, students are only allowed to use their devices when instructed to or in the designated areas.
- The students bring their devices into school on the understanding that it is at their own risk and they are responsible for their own device.
- The BYOD will be filtered so that certain websites and apps are inaccessible.
- Confiscation of devices and withdrawal of access to the BYOD network can be applied as a sanction for misuse.

Lesson Time

- In delivering the curriculum, there can be no expectation that students will have a device / smart phone. If Information Technology is a necessity then an IT suite should be used or the school tablets booked.
- Mobile / portable devices are only to be used within lesson time if permitted by the teacher in charge of the lesson.
- Students are not allowed to use cameras to film footage, capture photos or record audio of staff or fellow pupils without the express permission of a member of staff.
- When devices are in use within lessons, students are allowed to use them for the task set by the teacher, and must seek permission for other use.

Break / Lunch Times (and before / after lesson hours)

- Devices are allowed to be used at break / lunch times and before / after lesson hours in classrooms, the Hall and at all times in the library, Sixth Form study area, Sixth Form common room and outside. However it is still the case that no photography or filming is allowed without express permission of a member of staff.
- Students **ARE NOT** allowed to use their devices, or have headphones in, while walking through corridors of the school or whilst in the canteen.
- Audio from devices should be through headphones only.