Wallington High School for Girls
Online Safety Policy

Contents

1 **Aims and Rationale** 2
2 **Scope**....3
3 **Roles and responsibilities**....3
4 **Communication**....6
5 **Education and Curriculum**....6
6 **Expected Conduct**....7
7 **Incident Management**....8
8 **Managing the ICT Infrastructure**....9
9 **Data Security and transfer**....13
10 **Equipment and Digital Content**....13
11 **Training**....14
12 **Monitoring Arrangements**....15
13 **Links with other policies**....15

Appendices:

1. Student and Staff Acceptable Use Statement
2. Mobile Phone Policy

MONITORING AND EVALUATION BY	Senior Leadership Team and Headteacher
APPROVED BY	Local Governing Body
APPROVAL DATE	November 2023
EFFECTIVE DATE	November 2023
PERIOD OF REVIEW	3 years
DATE OF NEXT REVIEW	November 2026

Policy Notes
Policy may be subject to review and revision at any time by the Wallington Local Governing Body notwithstanding that the next review date has not been reached.

Review dates are for guidance only and whilst the intention is always to arrange reviews within the stated time frame all Policy Notes will remain in force until this has taken place and been formally approved by the Wallington Local Governing Body.

Wallington High School for Girls: Online Safety Policy

1. Aims and rationale of policy

Wallington High School for Girls believes that the use of information and communication technologies in school brings great benefits. Recognising the online safety issues and planning accordingly will help to ensure appropriate, effective and safe use of electronic communications.

This Online Safety Policy applies to all members of the school community (including staff, students, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

This policy together with the Student and Staff Acceptable Use Statement (GLT IT Policy, Appendix A), Anti-Bullying, Mobile Phone, Child Protection and Safeguarding, Behaviour for Learning Policy and Staff Code of Conduct is designed to keep staff and students safe in school when using ICT. This policy has been reviewed and informed by the DfE guidance 'Teaching Online Safety in School' (Jan 2023), 'Keeping Children Safe in Education' (Sep 2023), 'Cyber Security Standards for Schools and Colleges' (March 2023) and 'Filtering and Monitoring Standards for Schools and Colleges' (March 2023).

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;
- ensure that all students know how and to whom they report online safety issues to (as stated in the DfE 'Relationships Education, Relationships and Sex Education (RSE) and Health Education' page 27, Sep 2021).
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies;
- all members of the school community will be made aware of the need to report online safety issues/incidents;
- reports will be dealt with as soon as is practically possible once they are received;
- the Designated Safeguarding Lead/ Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks;
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures;
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the Local authority

This school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.

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.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and;

- **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

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 cyberbullying or other online 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. See the school's Behaviour for Learning Policy reference to Power of Search.

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

3. Roles and Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for online safety provision. • To take overall responsibility for data & 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 online safety roles and to train other colleagues, as relevant. • To be aware of procedures to be followed in the event of a serious online safety incident. • To receive regular monitoring reports from the Online Safety Lead/ DSL. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager).

Role	Key Responsibilities
Designated Safeguarding Lead/ Online Safety Lead	• The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place. • Has day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documentation. • Promotes an awareness and commitment to online safety throughout the school community. • Ensures that online safety education is embedded across the curriculum. • Liaises with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated. • Liaises with school ICT technical staff. • Communicates regularly with SLT and the designated Online Safety Governor to discuss current issues and review incident logs. • Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • Ensures that online 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 online safety issues and legislation and is aware of the potential for serious child protection issues to arise from online safety matters.
Governors / Online Safety Governor	• To ensure that the school follows all current online safety advice to keep students and staff safe • To ensure online safety education provision and staff training is taking place as intended. • To approve the Online Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in online safety activities. • The role of the Online Safety Governor will include an annual review with the Designated Safeguarding Lead/ Online Safety Lead. • To review (collated and anonymised) reports of online safety incidents.
Computer Science/ PSHCE Curriculum Leader	• To oversee the delivery of the online safety element of the Computer Science curriculum. • To oversee the delivery of the online safety element of the PSHCE curriculum. • To liaise with the Designated Safeguarding Lead/ Online Safety Lead on online safety matters as appropriate.
Teachers	• To embed online 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 teach students to be critically aware of the materials they read and ensure they are shown how to validate information before accepting its accuracy. • 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.

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's Online Safety Policy and guidance. • To read, understand and adhere to the school's Acceptable Use Agreement (Appendix 1) and Mobile Phone Policy (Appendix 2). • To be aware of online safety issues related to the use of mobile phones, cameras and personal devices and that they monitor their use and implement current school policies with regards to these devices. • To report any suspected misuse or problem to the Designated Safeguarding Lead/ Online Safety Lead. • To maintain an awareness of current online 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, and never through personal mechanisms, e.g. email, text, mobile phones etc.
GLT IT Team	• To report any online safety related issues that arise to the Designated Safeguarding Lead/ Online Safety Lead. • 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 Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant. • Ensure the use of the network / Virtual Learning Environment/ remote access / email is regularly monitored and report any misuse to the Designated Safeguarding Lead/ Online Safety Lead. • 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.
Students	• To read, understand and adhere to the school's Acceptable Use Agreement (Appendix 1) and Mobile Phone Policy (Appendix 2). • 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 and know how to do so. • 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 personal devices. • To know and understand school policy on the taking/ use of images and on cyberbullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and know that the school's Online 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 support the school in the creation / review of online safety policies.
Parents / carers	• To support the school in promoting online 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 adhere to the school's Acceptable Use Agreement (Appendix 1) and Mobile Phone Policy (Appendix 2). • To access the school website / MLE / online student records in accordance with the school's Acceptable Use Agreement. • To consult with the school if they have any concerns about their child's use of technology. • Monitor the use of their child's personal devices and how they use the internet outside of school.
External groups	• Any external individual / organisation will read an Acceptable Use Policy prior to consent or passwords being given to use any equipment or the internet within school.

4. Communication

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

- Policy to be uploaded to the school website and shared with staff and Governors.
- Sections of the policy to be included in the students' planners.
- 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.

5. Education and Curriculum

a. <u>Student Online Safety Curriculum</u>

This school has a clear online safety education programme as part of the Computer Science curriculum / PSHCE curriculum / assembly programme / enrichment programme / tutor time programme. The curriculum 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 website / 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 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 online '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 the receipt of inappropriate materials;
- to understand why and how some people will 'groom' young people online 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/carer, teacher or trusted member of staff, or an organisation such as ChildLine or the CLICK CEOP button.

b. <u>Parent Awareness and Training</u>

The school runs a rolling programme of advice, guidance and training for parents, including:

- information leaflets, in the Wallington Week and on the school website;
- annual online safety information evenings for parents;
- suggestions for safe internet use at home;
- signposting national support sites for parents.

6. 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 online safety practice when using digital technologies out of school and realise that the school's Online 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 personal devices. They should also know and understand school policies on the taking / use of images and on cyberbullying.

Staff:

- are responsible for reading the school's Online Safety Policy and using the school ICT systems accordingly, including the use of mobile phones, and personal devices;
- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school;
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications;
- staff should be expected to follow good practice when using personal social media regarding

their own professional reputation and that of the school and its community;

- users should immediately report to the Designated Safeguarding Lead/ Online Safety Lead – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Students:

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- users should immediately report to the Designated Safeguarding Lead/ Online Safety Lead – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

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.

7. Incident Management

In this school:

- there is a consistent application of the Online Safety Policy;
- 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 and when needed (e.g. the local authority, CEOP, UK Safer Internet Centre helpline) in dealing with online safety issues;
- monitoring, recording and reporting of online safety incidents take place and contributes to developments in policy and practice in online safety within the school;
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the school will contact the Police if one of our staff or students receives online communication that we consider as particularly disturbing or breaks the law.

- staff and students are given information about infringements of use and possible sanctions. Sanctions may include:
    - Detention;
    - Confiscation of the device;
    - Conversation with the Head of Year, Designated Safeguarding Lead/ Online Safety Lead and/or Headteacher;
    - Informing parents/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.

8. Managing the IT infrastructure

a. Internet access, security (virus protection) and filtering

This school:

- has the educational filtered secure broadband connectivity through Schools Broadband;
- uses a NetSweeper 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 are logged;
- has installed a monitoring system called Visigo that alerts any safeguarding concerns to the Safeguarding Team who will take any appropriate action necessary;
- ensures network health through use of Sophos anti-virus software;
- has blocked student access to music downloading 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' online use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas;
- ensures all staff and students accept and agree to an Acceptable Use Policy and understands that they must report any concerns;
- 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 websites;
- 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 Designated Safeguarding Lead/ Online Safety Lead and the IT Support Team;
- 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.

b. Network management (user access, backup)

This school:

- uses individual, audited logins 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 websites, where useful;
- ensures that storage of all data within the school conforms to the UK data protection requirements.

To ensure the network is used safely, this school:

- requires staff to read the school's Online Safety Policy;
- ensures that staff access to the school's management information system is controlled through the user's network account;
- provides students with an individual network login username;
- ensures all students have their own unique username and password which gives them access to the internet, the VLE and email account;
- makes clear that no one should log on as another user and 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;
- makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software 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 etc;
- 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 for 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;
- clarifies 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 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.

c. 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.

d. 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;
- 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:

This school:

- introduces students to email, and uses email as part of their Computer Science lessons;
- ensures 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 or threatening emails, but to keep them as evidence.

Staff:

This school:

- ensure that staff never use email to transfer staff or student personal data;
- ensures that staff know that emails 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.

e. 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 on 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.

f. Learning platform

- Uploading of information on the schools' VLE (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 school's VLE must 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 VLE.

g. Social networking

Staff should read this in conjunction with the provisions of the Student and Staff Acceptable Use

Statement (GLT IT Policy, Appendix A) and the Teachers' Standards Part Two.

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, parents / carers or school staff;
- they do not engage in online discussions 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.

h. 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.
- Our full CCTV Policy can be found on our website.

9. Data Security and transfer

Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to any illegal activity.

The school will conform with the GLT Data Protection Policy – see our website.

10. Equipment and Digital content

a. Personal mobile phones and devices

- Staff and students must adhere to the school's Acceptable Use Agreement (Appendix 1) and Mobile Phone Policy (Appendix 2) when using mobiles phones and personal devices, including laptops.
- Mobile phones and personal devices, including laptops, brought into school are entirely at the staff member, student and parents' own risk. The school accepts no responsibility for devices that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while students/ staff are travelling to and from school.
- The recording, taking and sharing of images, video and audio on any mobile phone or device is not permitted. All mobile phone use is to be open to scrutiny and the Headteacher has the right to withdraw or restrict authorisation for use at any time if deemed necessary.
- The school reserves the right to search the content of any mobile or device where there is a reasonable suspicion that it may contain undesirable material, including that which promotes pornography, violence or bullying. Staff mobiles or devices may be searched at any time as part of routine monitoring.
- 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.

b. Digital images and video

In this school:

- we gain parental / carer permission for the use of digital photographs or video involving their child as part of the school agreement form when their child 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 student 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 student 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 online 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 Computer Science scheme of work;
- students are advised to be very careful about placing any personal photos on any social media sites. They are taught to understand the need to maintain privacy settings so as not to make personal information public;
- 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.

c. Asset disposal

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

11. Training

This school:

- ensures staff/governors know how to send or receive sensitive and personal data;
- makes training and education on online safety issues available to staff and governors;
- provides, as part of the induction process, all new staff and governors with information and guidance on the Online Safety Policy and the school's Acceptable Use Policy and Mobile Phone Policy.

12. Monitoring

The school has an Online Safety Lead (Designated Safeguarding Lead) who is responsible for document ownership, review and updates.

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.

The Online Safety Policy has been written by the Designated Safeguarding Lead/ Online Safety Lead and is current and appropriate for its intended audience and purpose.

The governing body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals throughout the year.

The policy and has been agreed by the SLT and approved by Governors.

The school will monitor the impact of the policy using:

- logs of reported incidents
- monitoring logs of internet activity (including sites visited)
- internal monitoring data for network activity
- surveys/questionnaires of:
  - learners
  - parents and carers
  - staff.

13. Links with other policies

The Online Safety Policy should be read in conjunction with the following policies:

- Student and Staff Acceptable Use Statement (GLT IT Policy, Appendix A),
- Anti-Bullying,
- Mobile Phone,
- Child Protection and Safeguarding,
- Staff Code of Conduct
- Behaviour for Learning
- Data protection policy and privacy notices
- Complaints procedure

Appendix 1

Wallington High School for Girls

Acceptable use statement (for students and staff)

The IT and computer systems are owned by the Trust and are made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The Trust's Acceptable Use Statement has been drawn up to protect all parties - students, staff and the school.

By using the Trust IT network (and/or BYOD solution), staff and students agree to the Acceptable Use Statement.

- 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 Trust IT 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 the Trust. 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 Trust's IT Team;
- The Trust 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;
- Users are responsible for email they send and for contacts made that may result in inappropriate email being received. 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 Trust will not be held responsible for payment of any items ordered through the Internet, unless authorised by the Trust Finance Department;
- Other users' files must not be accessed;
- Students in the Trust will not give their home address or phone number to any person, nor use the internet to arrange to meet anyone, unless their parent/carer or teacher has given them permission.
- The use of memory sticks or any other form of removable storage is permitted. However, the user is responsible for checking said media for viruses before use.
- Data will be held in accordance with the Trust's Records Retention Policy. However, home folders, email accounts and other system access such as VLE and Office 365, will be removed from the Trust's systems 3 months after the users' leaving date.

For further and more comprehensive details relating to the use of the Trust's IT systems and equipment, please see the Trust IT Policy.

Appendix 2

Wallington High School for Girls

Mobile Phone Policy 2023-24

Students **are not** allowed to use their devices, or have headphones in sight, anywhere in the school unless directed by a teacher to use them for a specific task. If they are seen by a member of staff, they will be confiscated immediately and given to Reception.

When on school premises devices and headphones should be turned off and away. The exception to this rule is Year 12 and 13 who may use their devices in free classrooms, the Sixth Form study area, and the Sixth Form common room. **Devices must not be used in any other part of the school (e.g. corridors). Sixth Form students are reminded that they act as role models to the rest of the school.**

Year 7 and Year 8 students must not bring into school mobile phones or watches with internet access or a camera. Any students found with such devices will have them confiscated* and they will receive a 60 minute Centralised Detention. Parents/ carers will be informed.

* See confiscation below

Policy

Students and staff must be aware that:

- Students are not allowed to use cameras to film footage, capture photos or record audio of staff or fellow students without the express permission of a member of staff. Images of staff may not be shared under any circumstances.
- No student is allowed to upload to any external site any media footage taken in school (e.g. video, photos, audio, etc.) taken in school without express permission from the Headteacher.
- If students need to contact their parents/carers, and vice versa, they should speak to Reception. No direct communication with parents/carers is permitted.
- Sixth Form students may only listen to music (at a quiet level) using headphones in the Sixth Form Study Centre. However, students are strongly encouraged to avoid listening to audio when completing a task, as it reduces cognitive capacity. Students may not listen to music using headphones whilst completing a set task in class (e.g. revision).
- There can be no expectation that students will have a device when planning lessons and the use of a device should be avoided where possible. If it is necessary for students to use their device then this must be supervised closely and devices must be turned off immediately upon completion of task.
- Teachers must not set cover work which includes the use of a device. However, KS5 teachers may set work which requires the use of a device to access online resources.

Confiscation

Schools' general power to discipline enables a member of staff to confiscate, retain or dispose of a student's property as a disciplinary penalty, where reasonable to do so. Sixth Form students will be allowed to collect their confiscated device at the end of the day.

Stages

Stage 1: First offence

- The device is confiscated immediately and given to Reception who will add a negative point on Class Charts.
- Reception will inform parents/ carers that the device has been confiscated and of the next stage.
- Parents will be asked to collect the device from Reception by 4pm on that day. If a parent is unable to collect the device at this time the device will be stored securely until they can.

Stage 2: Second offence

- The device is confiscated immediately and given to Reception who will add a negative point on Class Charts and log a 60 minute Centralised Detention.
- Reception will inform parents/ carers that the device has been confiscated and of the next stage.
- Parents will be asked to collect the device from Reception by 4pm on that day. If a parent is unable to collect the device at this time the device will be stored securely until they can.

Stage 3: More than two offences

- The device is confiscated immediately and given to Reception who will add a negative point on Class Charts and log a Headteacher Detention.
- Reception will inform parents/ carers that the device has been confiscated and of the next stage.
- Parents will be asked to collect the device from Reception by 4pm on that day. If a parent is unable to collect the device at this time the device will be stored securely until they can.
- This will result in the student receiving a permanent ban from bringing their device to school for the remainder of the academic year.

Please note that in the case of serious breaches of this policy the school has the right to skip stages including the right to ban a student from bringing their device to school with immediate effect.

The school accepts no responsibility for devices that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while students are travelling to and from school.