



# Wimbledon College E-Safety Policy

## Contents

### 1. Introduction and overview

- Rationale and Scope
- Roles and responsibilities
- How the policy will be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

### 2. Education and Curriculum

- Pupil e-safety Curriculum
- Staff and governor training
- Parent awareness and training

### 3. Expected Conduct and Incident management

### 4. Managing the ICT infrastructure

- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Social networking

### 5. Data security

- Management Information System access
- Data transfer

### 6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

### *Appendices:*

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)

## 1. Introduction and Overview

### Rationale

#### The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Wimbledon College with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Wimbledon College.
- assist school staff working with children 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 relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- 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:**

### **Conduct**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

### **Contact**

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

### **Content**

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

### **Scope**

This policy applies to all members of Wimbledon College community (including staff, pupils, volunteers, parents/carers, visitors & community users) who have access to and are users of school ICT systems, both in and out of Wimbledon College.

The Education and Inspections Act 2006 empowers the Head Master to such extent as is reasonable, to regulate the behaviour of pupils 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 (refer to current DfE Guidance). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

## Roles and responsibilities

Role	Key Responsibilities
Head Master	<ul style="list-style-type: none"> <li>• To take overall responsibility for e-Safety provision</li> <li>• To take overall responsibility for data and data security (SIRO)</li> <li>• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements eg LGfL</li> <li>• To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant</li> <li>• To be aware of procedures to be followed in the event of a serious e-Safety incident.</li> <li>• To receive regular monitoring reports from the E-Safety Co-ordinator / Officer</li> <li>• To communicate regularly with the Designated Governor for Safeguarding to discuss current issues and to report any serious e-safety incidents</li> <li>• 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)</li> </ul>
e-Safety Co-ordinator / Designated Safeguarding Officer	<ul style="list-style-type: none"> <li>• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents</li> <li>• promotes an awareness and commitment to e-safeguarding throughout the school community</li> <li>• ensures that e-safety education is embedded across the curriculum</li> <li>• liaises with school ICT technical staff</li> <li>• To communicate regularly with SLT to discuss current issues, review incident logs and filtering / change control logs</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident</li> <li>• To ensure that an e-Safety incident log is kept up to date</li> <li>• facilitates training and advice for all staff</li> <li>• liaises with the Local Authority and relevant agencies</li> <li>• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> <li>• sharing of personal data</li> <li>• access to illegal / inappropriate materials</li> <li>• inappropriate on-line contact with adults / strangers</li> <li>• potential or actual incidents of grooming</li> <li>• cyber-bullying and use of social media</li> </ul> </li> </ul>
Governors / Safeguarding governor	<ul style="list-style-type: none"> <li>• To ensure that the school follows all current e-Safety advice to keep the children and staff safe</li> <li>• To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors/Governors Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor, within their role as Safeguarding Governor</li> <li>• To support the school in encouraging parents and the wider community to become engaged in e-safety activities</li> <li>• The role of the Safeguarding Governor will include:</li> </ul>

Role	Key Responsibilities
	<ul style="list-style-type: none"> <li>regular review of e-safety matters</li> </ul>
Computing Curriculum Leader	<ul style="list-style-type: none"> <li>To oversee the delivery of the e-safety element of the Computing curriculum</li> <li>To liaise with the e-safety coordinator regularly</li> </ul>
Network Manager / technician	<ul style="list-style-type: none"> <li>To report any e-Safety related issues that arises, to the e-Safety coordinator.</li> <li>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</li> <li>To ensure that provision exists for misuse detection and malicious attack (e.g. keeping virus protection up to date)</li> <li>To ensure the security of the school ICT system</li> <li>To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>the school's policy on web filtering is applied and updated on a regular basis</li> <li>LGfL is informed of issues relating to the filtering applied by the Grid</li> <li>that he / she keeps 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</li> <li>that the use of the network, remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Head Master for investigation / action / sanction</li> <li>To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.</li> <li>To keep up-to-date documentation of the school's e-security and technical procedures</li> </ul>
Registrar	<ul style="list-style-type: none"> <li>To ensure that all data held on pupils on the school office machines have appropriate access controls in place</li> </ul>
LGfL Nominated contact(s)	<ul style="list-style-type: none"> <li>To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>To embed e-safety issues in all aspects of the curriculum and other school activities</li> <li>To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant)</li> <li>To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws</li> </ul>
All staff	<ul style="list-style-type: none"> <li>To read, understand and help promote the school's e-Safety policies and guidance</li> <li>To read, understand, sign and adhere to the school staff Acceptable Use Agreement</li> <li>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</li> <li>To report any suspected misuse or problem to the e-Safety coordinator</li> <li>To maintain an awareness of current e-Safety issues and guidance e.g. through CPD</li> <li>To model safe, responsible and professional behaviours in their own use of technology</li> </ul>

Role	Key Responsibilities
	<ul style="list-style-type: none"> <li>• To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.</li> </ul>
Pupils	<ul style="list-style-type: none"> <li>• Read, understand, sign and adhere to the Pupil E-Safety and Acceptable use of ICT &amp; Social Media Agreement</li> <li>• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>• to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>• to know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>• to know and understand school policy on the use of mobile phones, digital cameras and hand held devices.</li> <li>• To know and understand school policy on the taking/use of images and on cyber-bullying.</li> <li>• 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</li> <li>• To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home</li> <li>• to help the school in the creation/ review of e-safety policies</li> </ul>
Parents	<ul style="list-style-type: none"> <li>• to support the school in promoting e-safety and endorse the school's Acceptable Use Agreement which includes the pupils' use of the internet and the school's use of photographic and video images</li> <li>• to read, understand and promote the school Pupil E-Safety and Acceptable use of ICT &amp; Social Media Agreement with their children</li> <li>• to access the school website/on-line pupil records in accordance with the relevant school Acceptable Use Agreement.</li> <li>• to consult with the school if they have any concerns about their children's use of technology</li> </ul>
External groups	<ul style="list-style-type: none"> <li>• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school</li> </ul>

## **Communication**

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and the staff intranet
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be kept in pupil's diaries and in personnel files

## **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 pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - Interview by the relevant member of staff
  - 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 LA / Police.
  - Sanctions in line with the School's Discipline Procedures
- Our e-Safety Coordinator 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 child protection procedures.

## **Review and Monitoring**

- The school has an e-safety coordinator 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
- There is widespread ownership of the policy and it has been agreed by the staff and SLT and approved by Governors and other stakeholders such as the FOWC. All amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

## 2. Education and Curriculum

### Pupil e-Safety curriculum

This school

- Has a clear e-safety education programme which covers a range of skills and behaviours appropriate to their age and experience, 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 pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign which they will be reminded of when a pupil logs on to the school network.
- 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 pupils 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 pupils 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;

### **Staff and governor training**

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education programme
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the eSafeguarding policy and the school's Acceptable Use Agreements.

### **Parent awareness and training**

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school web site;
  - demonstrations, practical sessions 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**

### **Expected conduct**

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign 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 policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying



### 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.

### Pupils

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

### Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school and the E-Safety agreement in their son's diary.
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

## **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, within its Behaviour Policy.
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the school's senior leaders,
- 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 pupils receives online communication that we consider is particularly disturbing or breaks the law

## **4. Managing the ICT infrastructure**

### **• Internet access, security (virus protection) and filtering**

#### This school:

- Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
- Uses the LGfL Net Sweeper 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 and only available to staff with the approved 'web filtering management' status;

- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc and network set-up so staff and pupils cannot download executable files;
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- 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;
- Uses security time-outs on Internet access where practicable / useful;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriately secure environment : the school's learning environment/ LGfL secure platforms such as J2Bloggy, etc
- Requires staff to preview websites before use [where not previously viewed or cached]; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required;
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the system administrator. Our system administrator(s) logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities.

- **Network management (user access, backup)**

This school

- Uses individual, audited log-ins for all users - the London USO system;
- 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;
- Has additional local network auditing software installed;
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage of all data within the school will conform to the UK data protection requirements

Pupils and Staff using mobile technology, where storage of data is online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide a different / use the same username and password* for access to our school's network;
- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- We provide pupils with an individual network log-in username. From Year 7 [Figures] they are also expected to use a personal password;
- All pupils have their own unique username and password which gives them access to the Internet, the student area on the school's network and their own school approved email account;
- We use the London Grid for Learning's Unified Sign-On (USO) system for username and passwords;
- Makes clear that no one should log on as another user and makes clear that pupils 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 pupils and one for staff. Staff and pupils 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 pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 8.00pm to save energy;
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- 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;  
e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- 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 and access is only through school / LA approved systems:  
e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;  
e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their username and password (their USO 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 our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- 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;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- 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.

### **Passwords policy**

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find. ;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use Strong passwords for access into our MIS system.
- We require staff to change their passwords into the MIS, LGfL USO admin site twice a year.

### **E-mail**

#### **This school**

- Provides staff with an email account for their professional use, *London Staffmail / LA email* and makes clear personal email should be through a separate account;
- Uses Londonmail with students as this has email content control
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example [info@schoolname.la.sch.uk](mailto:info@schoolname.la.sch.uk) / [head@schoolname.la.sch.uk](mailto:head@schoolname.la.sch.uk) / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils receives an e-mail 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 e mails dangerous. We use a number of LGfL-provided 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. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

### **Pupils:**

- We use LGfL LondonMail with pupils and lock this down where appropriate using LGfL SafeMail rules.
- Pupils' LGfL LondonMail e-mail accounts are intentionally 'anonymised' for their protection.
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils can only receive external mail from, and send external mail to, addresses if the SafeMail rules have been set to allow this.
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail 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 e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail 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 e-mail, 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 e-mail 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 e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

**Staff:**

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, named LA system;
- Staff know that e-mail 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. They are aware that:
  - 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;
- All staff sign our school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

**School website**

- The Head Master 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 web site 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 web site is the school address, telephone number and we use a general email contact address: [admin@wimbledoncollege.org.uk](mailto:admin@wimbledoncollege.org.uk). Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We expect teachers using' school approved blogs or wikis to password protect them and run them from the school website.

## **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 / pupils, 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.

## **Video Conferencing**

This school

- Only uses the LGfL / Janet supported services for video conferencing activity;
- Only uses approved or checked webcam sites;

## **CCTV**

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.
- We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

## **5. Data security: Management Information System access and Data transfer**

### **Strategic and operational practices**

At this school:

- The Head Master is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record



- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff,
  - pupils
  - parents
 This makes clear staffs' 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 and network access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertaken at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

### **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.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- Staff with access to the Admissions system also use a LGfL OTP tag as an extra precaution.
- We use RAv3 with its 2-factor authentication for remote access into our systems.
- We use LGfL's USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USOAutoUpdate, for creation of online user accounts for access to broadband services and the London content
- 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.
- All of our servers are backed up to onsite backup servers in a different building.
- We use LGfL's GridStore remote secure to back-up our SIMS server.

- 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 collected by secure data disposal service.

## **6. Equipment and Digital Content**

### **Personal mobile phones and mobile devices**

- Personally owned mobile phones and hand held devices brought into school are the responsibility of the staff member, pupils' & parents' or visitors and are brought in entirely at their own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school, including items confiscated in line with the school's Behaviour Policy.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Head Master. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Head Master 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.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone.
- Staff may use their phones during break times or in non-contact periods. If a staff member is expecting a personal call they may leave their phone with the school office/ PSA to answer on their behalf, or seek specific permissions to use their phone at other than their break times/non-contact periods.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms, swimming pool and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- 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.
- Sixth form pupils' 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.

### **Students' use of personal devices**

- Pupils in Years 7 to 11 are not allowed to bring mobile phones or personally owned devices into school. Sixth Form pupils are allowed to bring mobile phones and personal electronic devices into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. This has to be agreed with the pupil's Head of Line and the mobile phone must be left with the pupil's PSA while the pupil is in school.
- If there are exceptional reasons for a student to bring their personally own device[s] into to school they must have the permission of their Head of Line.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised to contact their son's PSA.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

### **Staff use of personal devices**

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones for contacting children, young people or their families within or outside of the school setting in a professional capacity, except in cases of emergency.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.

- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

## **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 son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, 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/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their eSafety 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;
- Pupils 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.
- Pupils 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 identify 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.

## **Asset disposal**

Details of all school-owned hardware is recorded in the school's asset tracking spreadsheet. 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](#). [Further information](#) can be found on the Environment Agency website.

Approved by Governing Body	17 <sup>th</sup> June 2015
Next Review Date	June 2016

## Appendices

### Appendix 1 - Acceptable Use Agreement (Staff)

## Wimbledon College Acceptable Use Policy - Staff agreement form

*This agreement covers use of all digital technologies in school, in relation to contact with pupils and parents and in relation to your professional responsibilities.*

*[i.e. email, Internet, intranet and network resources, website, software, equipment and systems]*

- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation, regular changing and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email, internet, intranet, network, or other school systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system for any school business.  
(This is currently the Lgfl staff mail)
- I will only use the approved school email, or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. Any communication system must be approved by the Head Master.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to my line manager / the Senior IT Technician.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role. I will ensure that all comments/entries/opinions made or expressed by me are clearly identified as my own and not those of the school.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.

- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named Safeguarding officer / relevant senior member of staff if I feel the behaviour of any child I teach may be a cause for concern.
- I understand that Wimbledon College may monitor usage of its internet and email services without prior notification or authorisation from users. All Internet usage and network usage can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff / named child protection officer at the school.
- I understand that failure to comply with this agreement could lead to disciplinary action, in line with the School's Disciplinary Procedure for teaching and support staff.

**User Signature**

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies. I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature: .....Date: .....

Full Name: ..... (printed)

Job title .....

**Authorised Signature [Head/Deputy]**

I approve this user to be set-up.

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

Full Name ..... (printed)

## Appendix 2 - Acceptable Use Agreement (Pupils)

### Pupil E-Safety Agreement and Acceptable Use of ICT

Wimbledon College has a curriculum computer network with full internet access to support learning. Boys can use this facility only when parents/guardians have signed this agreement.

[Advice: If you receive abusive messages: do not delete them, you do not have to read them but they may be used as evidence; ask for help from a trusted adult [e.g. parent/carer, teacher, PSA, etc] and do not forward a text, email, photo, video, etc. as you may make the problem worse. You may even be breaking the law.]

1. I will keep my login and password details secret.
2. I will only use the computers for school work and homework.
3. I will only use the internet with permission from the teacher in charge.
4. I will not use messaging software or clients.
5. I will use polite standard English in communications and good email etiquette at all times.
6. I will not give any personal details, including my address and telephone number or send photographs or videos that could be used to identify me unless expressly permitted by a member of staff.
7. I understand that my files will be checked and that my use of the internet will be monitored.
8. I will not undertake any activity, including loading software, that is found to threaten the integrity of the computer network or attacks or corrupts other systems.
9. I will respect the copyright of materials and software licence conditions.
10. I will not use any digital device to access, post or produce anonymous messages; material of an inappropriate, threatening, discriminatory, racist or offensive nature. I will not post derogatory or negative comments about the school or any member of the school community.
11. I will not post/upload on the internet or any social network any materials which can cause damage to my personal reputation, other people's reputation or the reputation of the school.
12. I will not post or upload any materials or photos which can identify the school and breach the safety of our pupils on any social network such as YouTube/ Facebook/ MSN/ Twitter/Snapchat /etc. I will respect the required age to create accounts on social networks.
13. I will respect the school computer hardware and not abuse it.
14. I will report to any member of staff, any videos or materials, showing the school buildings or students in uniform, posted on the web, or social networks, without the school's permission.
15. I am aware that breaching any of the above will be subject to an appropriate sanction, which may result in withdrawal of internet access in school and ultimately in exclusion.

Pupil's Signature: \_\_\_\_\_

Date: \_\_\_\_\_

As the parent/carer of the student signing above, I grant permission for my son to use email and the internet. I understand that pupils will be held accountable for their actions. I also understand that some materials on the internet may be objectionable and I accept joint responsibility for the setting of standards for my son to follow when selecting, sharing and exploring information and media.

Parent/Carer's Signature: \_\_\_\_\_ Date \_\_\_\_\_