Fulham SCHOOL

ESAFETY AND USE OF ICT POLICY

Reviewed by:	**Will le Fleming**	**March 2019**
Confirmed by:	**Executive Group**	**8 March 2019**
Approved:	**Board of Governors**	**14 March 2019**

Next review: September 2020

Contents

1. INTRODUCTION

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

Fulham School will deal with e-Safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, including:

- The Child Protection and Safeguarding Policy
- Behaviour, Sanctions and Rewards Policy
- Anti-Bullying Policy
- Staff Handbook
- Staff Code of Conduct

It will, where known and appropriate, inform parents of incidents of inappropriate eSafety behaviour that take place out of school.

2. ROLES AND RESPONSIBILITIES

Governors
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. Specific responsibilities include:

- Regular monitoring of e-Safety incident logs
- Regular monitoring of filtering systems
- Discussion of eSafety at relevant Governors' meetings

Executive Group and management teams
All members of the Executive Group (the Headmaster, Head of Prep, Head of Pre-Prep and School Business Manager) have a duty of care to ensure the safety (including e-Safety) of members of the school community, supported by their respective management teams. Many of the day-to-day responsibilities for e-Safety are in the hands of the IT Manager with the support of the IT Steering Group.

IT Manager
The IT Manager is responsible for ensuring the following:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the School meets all e-Safety technical requirements
- That users may only access the school's networks and devices if properly authenticated and authorised.
- That the filtering policy is applied and updated on a regular basis.

- That they keep up to date with e-Safety technical information in order to carry out their e-Safety role effectively and to inform and update others as relevant.
- That the use of the school's networks and devices is regularly monitored to ensure compliance with the Acceptable Use Policies (AUPs) in order that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation.
- That monitoring software and systems are kept up to date.

Teaching and Support Staff
Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-Safety matters and of the current e-Safety policy and practices.
- They have read, understood and agreed to the Staff AUP agreement.
- They report any suspected misuse or problem to the appropriate person for investigation.
- All digital communications with other staff, pupils and parents are on a professional level.
- They help pupils understand and follow the e-Safety and acceptable use policies.
- They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Designated Safeguarding Leads
Designated Safeguarding Leads are trained in e-Safety issues and made aware of the potential for serious child protection and safeguarding issues to arise from:

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

Pupils
Pupils are responsible for using the school digital technology systems in accordance with the Pupil AUP Agreements. All pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

In addition pupils:

- Are expected to know and understand policies on the use of mobile devices and digital cameras.
- Should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-Safety practice when using digital technologies out of school and realise that the school's e-Safety Policy covers their actions.

Parents
Parents play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. Parents are asked to support the school in promoting good e-Safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to the intranet
- Their children's personal devices in the school

Community Users
Anyone who accesses school systems as part of the wider school provision will be expected to sign a Visitors' AUP agreement before being provided with access to school systems.

3. GENERAL PRINCIPLES

ICT technologies allow access to an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

e-Safety should be a focus in all areas of the curriculum and staff should reinforce e-Safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, and will be provided in the following ways:

- An e-Safety curriculum is provided as part of ICT, PSHE and other lessons and is regularly revisited
- Key e-Safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils are helped to understand the need for the Pupil AUP agreement and encouraged to adopt safe and responsible use both within and outside school
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging
- Pupils are made aware of the impact of cyber-bullying. See also the Child Protection and Safeguarding Policy
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, older pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT Support to remove those sites from the filtered list for those pupils. Any request to do so should be audited by the IT Manager, and clear reasons for the need must be established and recorded.

Parents play an essential role in the education of their children and in the monitoring / regulation of children's on-line behaviours. The School provides information and awareness to parents through seminars and other methods as appropriate.

It is essential that all staff who are granted access to the school network receive e-Safety training and understand their responsibilities, as outlined in this policy. Training will be arranged and overseen by the Executive Group and management teams, and recorded as having taken place, as follows:

- e-Safety training is made available to staff. This is regularly reinforced.
- All new staff receive e-Safety training as part of their induction programme, ensuring that they fully understand the school e-Safety and Use of ICT Policy.

The IT Manager will receive regular updates through attendance at external training events and/or by reviewing guidance documents released by relevant organisations.

4. SYSTEM AND TECHNICAL INFORMATION

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements. The IT Manager continually reviews and audits the safety and security of school technical systems.

Servers, wireless systems and cabling must be securely located and physical access restricted. Data is backed up nightly and securely encrypted.

Internet access is filtered for all users via Smoothwall. The firewalls check for an updated filter list daily. If a URL is not on the filter list, the firewall checks the manufacturer's database directly. This database is updated constantly.

The school provides user-level filtering, allowing different filtering levels for different ages and different groups of users from Pre-Prep to staff.

All pupil web access is logged. Staff web access to restricted categories is also logged. Users are made aware of this in the AUP agreement. If a site is blocked by the filter as being inappropriate then access is not allowed. A report on such attempts reviewed by senior staff and any concerns discussed at management team level.

Security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts that might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date anti-virus and anti-malware software.

5. SECURITY

All users are provided with a username and required to set a secure password. Users are responsible for the security of their username and password.

Passwords must:

- Be a minimum of 10 characters in length
- Contain characters from three of the following four categories
    - Uppercase characters (A through Z)
    - Lowercase characters (a through z)
    - Numerical Digits (0 through 9)
    - Wildcard character (for example # or $ or % or !)

Passwords must not contain the following:

- Patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Common words spelled backward or preceded or followed by a number (for example, 'terces', 'secret1' or '1secret').
- Standard words or phrases such as 'Welcome123', 'Password123' or 'Changeme123'

Passwords will expire every 90 days and require reset. Further guidance on secure password creation may be obtained from the IT Manager.

Passwords must be kept secure:

- One of the most common forms of password compromise is storing the details in an insecure location or writing it down on a piece of paper that is easily accessible or visible.
- Do not store your login credentials on your computer, mobile device or phone on software that is easily accessible.
- Do not write your password down in a book or on paper and store it at your desk or stick a note to your monitor or computer screen.
- Do not supply or share your work password or login credentials with anyone.

Staff must ensure that any school information accessed from their PCs or removable/portable media equipment is kept secure.

Staff should lock screens before moving away from their computers to prevent unauthorised access. Screens should be kept out of view of pupils or third parties when accessing personal, sensitive, confidential or classified information

Staff should avoid leaving any portable or mobile IT equipment or removable storage media in unattended vehicles or classrooms. Where this is not possible, keep it locked out of sight.

Staff should always carry portable and mobile IT equipment or removable media as hand luggage, and keep it under control at all times.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.

No sensitive or confidential information should be left openly in staff work areas. Such materials should be securely stored under lock and key.

More generally the following areas describe some of the most typical threats to the security of ICT systems and data. All staff should make careful note of the advice contained here.

Social Engineering and Phishing Scams
Social engineering and phishing scams are a major source of compromised account credentials. These are eternal attacks that trick the user to reveal their account information. These attacks can be via phone, text or email. A common form of attack is a disguised email that looks legitimate requesting a user to reset or provide account login credentials. The email could contain a link or fraudulent login page directing the user to provide login credentials. In some cases the link may contain embedded malicious code that gets installed on the user's computer.

Users must not provide any account authentication credentials (both account login name and password) via email or text. Users must not reset account credentials via website links other than those systems that are solely used by Fulham School.

Brute force attacks
Dictionary and 'Brute-force attacks' are techniques used by attackers to guess insecure passwords to gain access to a system. Passwords that are generated or created poorly are the most susceptible to being compromised. Users must not use easily guessed passwords such as pet's names or common words, etc.

Public kiosks or untrusted devices
Credentials are at high risk when used on public kiosks (hotels, airports, etc.) and on untrusted devices (friends or family devices). You may forget to logout and the next user may obtain your credentials; or the device may have already been compromised with malware that can obtain your credentials. Do not login to School systems from public kiosks or untrusted devices.

Shoulder surfing
Someone may be observing you logging in through your computer or mobile device and record your credentials. High risk areas are any location outside of the office, such as libraries, airports, hotels and public areas. Be vigilant when accessing your accounts and do not assume that you are safe from compromise.

Cross-referencing
Attackers obtain credentials from multiple forms of software or devices and engineer your login credentials to gain access to systems. An example of this is using the same password across multiple systems, such as Facebook, Twitter, email, etc. Do not use your School account

password on any other system or device. You should use unique credentials for all systems you access.

Malicious software
Attackers obtain account credentials through software attacks such as Malware on computers or 'key loggers' on websites to record account credentials.

- Do not install suspicious software onto your computer or mobile device.
- Do not open suspicious emails, links or attachments within suspicious emails.
- Keep your anti-virus software updated on a regular basis and do not disable anti-virus software.
- Keep your computer operating system updated on a regular basis and do not prevent operating system updates from occurring.

Sniffing attacks
All websites that require login credentials to be used must have a Secure Socket Layer (SSL) certificate from a legitimate source such as Verisign, Thawte, GeoTrust, GoDaddy, etc. Any website that does not have a SSL certificate installed (making it insecure) means that your login credentials are passed in the clear and an attacker can read this information by 'sniffing', when you login to insecure sites. Ensure that you are not inadvertently using an insecure of false site when entering login details.

6. BRING YOUR OWN DEVICE (BYOD)

Users who connect their own devices to the school's network (permitted from Year 7 in the Pre School and throughout the Senior School) are bound by the school's policies and accept the relevant AUP agreement. The School adheres to the principles of the Data Protection Act.

All school network systems are secure and a username and password is required to access the wireless network. Devices connected to the school's network are covered by the school's normal filtering systems.

Pupils receive guidance on the appropriate use of personal devices.

7. USE OF DIGITAL AND VIDEO IMAGES

The taking, storage and use of images is an important aspect of the use of ICT. All pupils and staff should be aware of the potential sensitivities in this area, and the implications for both safeguarding and data privacy. Please see the Taking, Storage and Use of Images Policy for more details.

In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use, but these images should not be published on social media or other channels.

8. COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance both teaching and learning. However, the School seeks to ensure that appropriate usage guidelines are in place, and that appropriate education is in place, to mitigate the potential negative consequences of some communication technologies.

In accordance with the AUP agreement, users must immediately report 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. Pupils report to an adult – usually their form teacher of head of year. Staff report to the IT Manager or any senior member of staff.

Pupils are taught about e-Safety issues, such as the risks attached to the sharing of personal details. They are reminded of the need to communicate appropriately when using digital technologies.

Pupil mobile phones
Mobile phones may be brought to school from Year 6. From Year 6 to Year 9 phones must be handed in to form teachers in the morning and reclaimed before going home. In Year 9 teachers may authorise the temporary use of phones to support learning projects.

From Year 10 upwards pupils are permitted to retain their mobile phones all day. However, they may not be used in various areas of the school or at various times of day as directed by teachers. In addition regular phone-free days or sessions are instigated to help manage usage.

Use of email
The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be it staff-based or pupil-based, within school or international. We recognise that pupils need to understand how to create an e-mail in relation to their age and ensuring proper network etiquette.

All children from the start of the Prep School (Year 3 upwards) have their own email address and are guided in its use. The school email service may be regarded as safe and secure. Users should be aware that email leaving or entering the school is scanned for viruses, spam and bad language.

Managing e-Mail

- The school gives all staff their own e-mail account to use for all school business as a work-based tool.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your school role may be subject to disclosure in response to a request for information. You must therefore actively manage your e-mail account as follows:
    - Delete all e-mails of short-term value
    - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- You should therefore take care not to send anything via email that may reflect badly on the School. In particular, you must not send content of a sexual, racist or discriminatory nature, junk mail, chain letters, cartoons or jokes from any email address associated with work.

Sending e-Mails

- Use your own school e-mail account so that you are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- School e-mail is not to be used for personal advertising and any personal communication via school e-mail should be kept to a minimum

Receiving e-Mails

- Check your e-mail regularly
- Activate your 'out-of-office' notification when away for extended periods
- Never open attachments from an untrusted source; consult the IT manager first
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- The automatic forwarding and deletion of e-mails is not allowed
- Respond to emails in a timely fashion

e-mailing Personal, Sensitive, Confidential or Classified Information

Where your conclusion is that e-mail must be used to transmit such data:

- Obtain express consent from your line manager to provide the information by e-mail
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Verify the details, including accurate e-mail address, of any intended recipient of the information
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document attached to an e-mail
- Provide the encryption key or password by a separate contact with the recipient(s)
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

9. SOCIAL MEDIA

The school encourages and supports staff in their use of digital technologies, sites and apps in the course of their work (teaching, extracurricular, pastoral) with pupils but requires that any such use is informed and fully consistent with our standards and policies. All staff must read and make sure they understand the staff Handbook and Code of Conduct before engaging in any such activity.

It is crucial that students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and other staff and the reputation of the school are safeguarded.

Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

This guidance applies to the governing body, all teaching and other staff, external contractors providing services on behalf of the school, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members'. The guidance covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school.

Key principles

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
- You must not engage in activities involving social media that might bring Fulham School into disrepute.
- You must not represent your personal views as being those of Fulham School on any social medium.

- You must not discuss personal information on social media about students, school staff and other professionals you interact with as part of your job.
- You must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations, or the School.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Fulham School.

Personal use of social media

- Staff members must not identify themselves as employees of Fulham School or service providers for the School in their personal webspace or any form of social media. This is to prevent information on these sites from being linked with the School and to safeguard the privacy of staff members.
- Staff members must not have contact through any personal social medium with any student from Fulham School unless the student is a family member.
- Staff members must not have any contact with students' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
- If staff members wish to communicate with students through social media sites or to enable students to keep in touch with one another, they can only do so with the approval of the school and through official school sites.
- Staff members must decline 'friend requests' from students they receive in their personal social media accounts.
- Staff members must not communicate with former students through social media sites until they are adults and in the case of Fulham Senior pupils until three years have passed since they left the School.
- On leaving Fulham School's service, staff members must not contact our students by means of personal social media sites. Similarly, staff members must not contact students from their former schools by means of personal social media.
- Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues, and other parties and school financial and operational information must not be discussed on their personal webspace.
- Photographs, videos or any other types of image of students and their families or images depicting staff members wearing school uniforms or clothing with school logos or images must not be published on personal webspace.
- School email addresses and other official contact details must not be used for setting up personal social media accounts, voucher and marketing unless permission is granted by SMT for the purpose of school matters, or to communicate through such media.
- Staff members must not edit open access online encyclopaedias such as Wikipedia in a personal capacity at work. This is because the source of the correction will be recorded as the School's IP address and the intervention will, therefore, appear as if it comes from the School itself.
- Fulham School logos or brands must not be used or published on personal webspace.

- Fulham School only permits limited personal use of social media while at work. Access to social media sites for personal reasons is not encouraged and all staff are requested to access these sites within their own time. Staff members are expected to devote their contracted hours of work to their professional duties.
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Using social media on behalf of Fulham School

- Staff members can only use official school sites for communicating with students or to enable students to communicate with one another.
- There must be a strong pedagogical or business reason for creating official school sites to communicate with students or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.
- Official school sites must be created only according to the requirements specified in this policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.
- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- In the case of a staff member being provided permission to create a school-related internet page, site, or channel on social media: on their exit from employment at Fulham School all security details for such sites must be passed over to the management team or relevant member of staff.

Breaches of Social Media guidance

- Any breach of this guidance may lead to disciplinary action being taken against the staff member/s involved in line with the school's Disciplinary Policy and Procedure.
- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Fulham School or any illegal acts or acts that render the school liable to third parties may result in disciplinary action or dismissal.
- Contracted providers of Fulham School services must inform the IT Manager immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school. Any action against breaches should be according to contractors' internal disciplinary procedures.

10. UNSUITABLE USER ACTIONS

Some actions are unsuitable for all ICT users and illegal. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images: the making, production or distribution of
- indecent images of children. Contrary to The Protection of Children Act 1978
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008
- Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986

Additionally the following actions/content are unsuitable for all users:

- Statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity
- Pornography & adult material
- Promotion of any kind of discrimination
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass deliberately the filtering or other safeguards employed by the school
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- On-line gambling
- File sharing (peer-to-peer)

Online gaming by pupils may be permitted, particularly for example where the content is educational, though such usage is carefully overseen and monitored by appropriate staff. The same applies to use of social media and messaging apps.

11. RESPONDING TO INCIDENTS OF MISUSE

Reports of misuse of IT equipment and services may originate from a variety of sources, including reports of concerning behaviour. However the incident is reported or discovered there are two broad courses of action that will be taken depending entirely on whether there is any suspicion of illegality involved or not.

Illegal Incidents
Anyone suspecting that:

- access has been attempted to any website containing child abuse images
- access has been attempted to any website containing material that breaches the Obscene
- Publications Act
- access has been attempted to any website containing criminally racist material
- access has been attempted to any website which contains statements or images that are
- intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activity

and anyone discovering any circumstance where any such materials are themselves to be found on any electronic device - whether owned by the School or not - or where there has been any incident by electronic means of 'grooming' behaviour must report all allegations, complaints, concerns or suspicions directly to the Headmaster or, in his absence, to the Chairman of Governors, unless that person is the subject of the concern. Concerns about the Headmaster should be reported to the Chair of Governors (or in his absence, the Vice Chair). All allegations, complaints, concerns or suspicions about the Chair of Governors should be reported to the LADO without the Chairman of Governors being informed.

Please see the Child Protection and Safeguarding Policy for more details and a reporting summary.

Concerns, suspicions or allegations of other IT related illegal activity (such as fraud, copyright theft or unlicensed use of software) by a member of staff should also be reported according to the reporting hierarchy outlined above. Such concerns will be managed in accordance with the School's Whistleblowing Policy.

Concerns that relate to the illegal behaviour or actions of pupils or parents (and not staff) should be reported to the DSL or Deputy DSL (DDSL). The DSL or DDSL will follow the Child Protection and Safeguarding Policy and in reporting any such behaviour to Children's Social Care and/or the Police.

Suspicions of other IT-related illegal activity (such as fraud, copyright theft or unlicensed use of software) should be reported directly to the IT Manager for pupils of the Headmaster for members of staff

Other Incidents
Reports of misuse of IT equipment and services that do not raise safeguarding concerns, nor appear to suggest any other kind of illegal activity, should be made directly to the appropriate Line Manager (usually the Head of Department) who will take action as appropriate, consulting the IT Manager as necessary to establish, capture and preserve any relevant data or other evidence.

Misuse of IT equipment and services by pupils or visitors should be referred first to the IT Manager who may refer to a senior member of staff as appropriate.

Should any of these investigation uncover materials or accesses for which there is any suspicion of illegality the IT Manager staff will immediately suspend any further inspection, reporting the matter in accordance with the procedure above (illegal incidents) or to the Police (if already involved) and awaiting direction from them.

Fulham
PRE-PREP

ICT Acceptable Use Agreement

This agreement is intended to encourage the imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The School provides both networked, desktop computers and wireless access to the internet through its own filtered connection. Wireless access is available everywhere in the school for pupils to use if given permission to do so.

- I will only use IT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher or TA
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher or someone in the IT Department immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of IT can be checked and that my parent may be contacted if a member of school staff is concerned about my eSafety.

I agree to comply with the rules and regulations set out in the Fulham Pre-Prep ICT Acceptable Use Agreement.

ICT Acceptable Use Agreement

This agreement is intended to encourage the imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The School provides both networked, desktop computers and wireless access to the internet through its own filtered connection. Wireless access is available everywhere in the school for pupils to use if given permission to do so.

Personal safety and responsibility

- I understand that the School will log and monitor my use of computers, devices and my digital communications;
- I will keep my school username and password safe and secure. I will not share it, nor will I try to use another pupil's or staff member's username and password. I understand that I should not write down or store passwords where it is possible that someone may steal them;
- I will not leave any school device, or device connected to the school network, logged on for others to use;
- I will not give out personal information about myself or others that could be used to identify me, my family or my friends (e.g. addresses, email addresses, phone numbers, information about the school or my age or the age of another pupil) unless a trusted adult has given me permission;
- I will never arrange to meet someone I have only ever previously met online unless I take a trusted adult with me;
- I will only use school computers and devices as directed. I will not use school devices for on-line gaming, online gambling or internet shopping and I will not visit sites I know to be unsuitable;
- I understand that some websites and social networks have age restrictions and I will respect this;
- I understand that once something is posted online or written in an email it has a permanence that is not like something that is said. It can be repeated, is searchable and can be copied out of context. I understand that I have to take responsibility for my actions online and I should consider my reputation, the reputation of others and the reputation of the School.
- If I see anything unpleasant or inappropriate or I receive a message I do not like, I will not respond but I will save it and talk to a trusted adult as soon as possible;
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language. I will not send messages either anonymously or pretending to be someone else and I will not send group messages needlessly;

- I will not take or distribute images of anyone without their permission
- I will edit or delete my own files only and not view, or change other people's files without their permission.

Device security

- I will only use my personal devices (mobile phone, USB device, laptop , iPad etc.) in school if I have been authorized by a member of staff and explicit permission has been granted to bring in the device to facilitate teaching and learning. I understand that if I do use my own devices in school I will follow the rules set out in this agreement, in the same way as if I were using school equipment;
- I will not try to upload, download or access any materials which are illegal, or encourage illegal, extremist or terrorist activity, or which may cause harm or upset to others, nor will I try to use any programs or software that might allow me to bypass the filtering systems in place to prevent access to such materials;
- I will report immediately any damage or faults involving school equipment or software, however this may have happened;
- I will report any actual or potential technical incident or security breach to the Head of Computing;
- I will not open a hyperlink in any email or attachment to an email if I have any concerns about it or think it may contain a virus or other harmful program;
- I will not install, attempt to install or store programs or software on any school device, nor will I try to alter the computer settings.

Sanctions

I understand that if I fail to comply with this Acceptable Use Agreement I will be subject to disciplinary action. This would include involvement in incidents of cyber-bullying or any inappropriate behaviour that is covered in this agreement, when I am in or out of the School and where it involves my membership of the school community.

I agree to comply with the rules and regulations set out in the Fulham Prep ICT Acceptable Use Agreement.

Fulham
SENIOR

ICT Acceptable Use Agreement

This agreement is intended to encourage the imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The school provides both networked, desktop computers and wireless access to the internet through the school's own filtered connection. Wireless access is available for use via your own devices. It is standard practice in organisations to audit users' internet activity and all staff and pupils are audited in this way. Audit trails are examined when necessary. Should you find yourself looking at or opening material you consider the school would think inappropriate (or material you find disturbing), simply inform a member of staff so we can work with you to address the matter.

I understand that the school will log and monitor my use of computers, devices and my digital communications.

Identity and responsibility (online and digital)

This section applies to all your use of digital technologies, whether school-owned or personal. In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

- I will be a responsible user and stay safe when using the internet and other digital technology at school.
- I will ensure that my online activity or use of mobile technology, in school or outside, will not cause my school, the staff, students or others distress or bring the school into disrepute.
- I will respect and maintain the integrity of my own and others' digital identities
- I will log on only as myself
- I will keep my login details private and make them secure
- I will not leave any device logged in and accessible to others
- I will exercise informed judgement about disclosing my personal details and will not give out another person's details without their clear consent
- I will be polite and responsible when I communicate with others.

- I will never arrange to meet someone I have only ever previously met on the internet or by e-mail or in a chat room, unless I take a trusted adult with me
- I will not make, post or send images and video footage of others except with the agreement and understanding of those involved. Agreement must extend to the finished, edited product
- I will respect my body and other people's – part of that means using positive words about myself and others; it also means not revealing too much on camera and not sharing or posting inappropriate photos.
- I understand that many apps have geolocation settings (identifying my location or where I made a post or took a photo). I will make sure that I know how to turn geolocation on and off, and not tell the world where I am at all times or make it too easy to find out where I live or go to school.
- I understand that financial transactions are permitted provided that I act within the constraints of the school's rules and with my parents' approval.
- I understand that the school's computers and systems are not to be used to upload, download or access any materials which are illegal, or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or likely to cause harm or distress to others, or bring the school's name into disrepute. I understand that I may not use any program or software to access such materials by bypassing the school's filters.

Network and hardware integrity

- I will respect and maintain the network and the computers the school provides:
- I will not open unexpected or suspicious files.
- I understand the need to exercise judgement when connecting a device to the school's network or to a computer. Those with non-executable files on them are clearly fine, but those with executables (e.g. a browser designed to run safely from a USB stick) can be harder to assess. I will not store or seek to install any executable file on the school network.
- I will not link devices that are themselves computers (in whatever form) to the wired network without first consulting either the Head of Computing or the IT Manager.
- I understand the need to exercise judgement when downloading files and am aware that viruses can be hidden in documents and images (for example) and not just in executable files. I will always seek advice if in doubt.
- I will respect the network's integrity when sending messages. I will not spam people or send needless messages. I will not attempt to send messages anonymously or pseudonymously for malicious purposes.
- I will report any actual or potential technical incident or security breach to the Head of Computing.
- I understand that if I fail to observe this agreement I will be subject to disciplinary action.

I agree to comply with the rules and regulations set out in the Fulham Senior ICT Acceptable Use Agreement.

ICT Acceptable Use Agreement for staff at Fulham School

This agreement is intended to encourage the imaginative, responsible and safe use of digital technologies. By acting with care and thought you should be putting into practice much of this policy.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use when in school, when using school systems and equipment and when connected to the school network
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that staff are protected from potential risk in their use of ICT in their everyday work

Access to ICT is made available to staff to enhance their work and to enhance opportunities for pupils' learning, and the School expects staff to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.
- In any interactions with pupils I will ensure appropriate use of ICT.
- I confirm that I have read and understood the Fulham School e-Safety and ICT Use Policy.

For my professional and personal safety:

- I understand the school will monitor my use of its ICT systems and networks.

- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school, and to the transfer of personal data out of school.
- I understand that the security of my account is my responsibility and that I should
- Log on only as myself;
- Keep my login details private and make them secure;
- Not leave any device logged in and accessible to others.
- I will report any actual or potential technical incident or security breach to the IT Manager.
- I will immediately report any illegal, inappropriate or harmful material I become aware of when in school or connected to the school network:
- Material that appears to originate from sources external to the School should be reported to IT Support;
- Material that appears to have been sent or circulated by a pupil or parent should be reported to the DSL or DDSL;
- Material that appears to have been sent or circulated by a member of staff (including a temporary member of staff or volunteer) should be reported to the Headmaster.

I will be professional in my communications and actions when using school ICT systems at school, when using school ICT systems and equipment or when connected to the school network:

- I will ensure that when I take and / or publish images of others I will do so in accordance with the school's policy on the use of digital / video images.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- Any use that I make of chat and social networking sites will be in accordance with the guidance given in the staff handbook and Code of Conduct.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I understand that the school ICT systems are primarily intended for educational use.

The school has the responsibility to provide safe and secure access to ICT:

- I will not open any hyperlinks in emails, or any attachments to emails, unless the source is known and trusted.
- I will not try to upload, download, or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access such materials.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Data Protection Policy.
- I understand that data protection requires that any staff or pupil data to which I have access must be kept private and confidential.

- I will immediately report any damage, loss or faults involving school equipment or software to IT Support.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this AU Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises
- I am aware that emails may be disclosed as evidence in court and that, even if deleted, copies may exist on a back-up system
- I understand that if I fail to comply with this AU Agreement, I could be subject to disciplinary action.

I agree to comply with the rules and regulations set out in the ICT Acceptable Use Agreement for staff at Fulham School.

ICT AUP Agreement for visitors to Fulham School

- I understand that I must use the school's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.
- I understand that my use of the school's systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- Whilst in the school, I will not try to upload, download or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the IT Manager.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove, add to or otherwise alter any other user's files, without permission.
- I will not install or attempt to install programs of any type on a school device, nor will I try to alter school computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the IT Manager.

I understand that if I fail to comply with this agreement the school has the right to remove my access to school systems and devices.

I agree to comply with the rules and regulations set out in the ICT Acceptable Use Agreement for visitors to Fulham School

Appendix 5: Guidance on creating social media sites on behalf of Fulham School

Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Fulham School.

Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

The proposed audience and level of interactive engagement with the site, for example whether students, school staff or members of the public will be able to contribute content to the site, must be discussed with the school's IT Manager, Head of Computing Curriculum and SLT.

Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

The site proposer must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school's brand and image.

Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

The guidance in this appendix applies equally to sites proposed by pupils at Fulham Senior. Staff may delegate some of the activities in this guidance to pupils but retain control and oversight as indicated here.

Children and young people

When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.

If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, the DSL or

DDSL must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

Staff members must also ensure that the webspaces they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.

Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from the SMT and/or appointed manager.

Approval for creation of or participation in webspace

- Fulham School social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Fulham School employees.
- Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the SLT, as must approval for participating on behalf of Fulham School on sites created by third parties.
- Content contributed to own or third-party hosted sites must be discussed with and approved by the SLT, and/or appointed manager.
- The school's SMT must be consulted about the purpose of the proposed site and its content, and approval must be obtained for the use of the school logo and brand.
- Staff must complete the Social Media Site Creation Form in this guidance and forward it to the SMT before site creation.
- Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Head immediately. Staff members must not communicate with the media without the advice or approval of the Head.

Content of webspace

- Fulham School hosted sites must have clearly expressed and publicised Terms of Use and 'House Rules'. Third-party hosted sites used for work purposes must have Terms of Use and 'House Rules' that conform to the school's standards of professional conduct and service.
- Staff members must not disclose information, make commitments or engage in activities on behalf of the school without authorisation.
- Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school's image, reputation and services.
- Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law apply to the content of social media.
- Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

- Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.
- Fulham School hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.
- Staff members participating in Fulham School hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.
- Staff members must never give out their personal information such as home contact details or home email addresses on these sites.
- Personal opinions should not be expressed on official sites.

Contributors and moderation of content

- Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.
- Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.
- The content and postings in Fulham School hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.
- The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the Terms of Use and House Rules. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.
- For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.
- Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and the appropriate member of senior staff informed.
- Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the House Rules must not be posted or removed. No one outside the school community is permitted to be a friend of the site.
- Any proposal to use social media to advertise for contributors to sites must be approved by the SLT.
- Approval must also be obtained from the SLT to make an external organisation a 'friend' of the site.

Fulham School Social Media Site Creation Form

Use of social media on behalf of Fulham School must be approved prior to setting up sites. Please complete this form and forward it to the SLT.

TEAM DETAILS	
Department:	
Author of site:	
Author's line manager:	
PURPOSE OF SITE	
What are the aims you propose to achieve by setting up this site? What is the proposed content of the site?	
PROPOSED AUDIENCE **Please tick all that apply.**	
☐ Pupils of Fulham School (specify age range) ☐ Fulham School staff ☐ Pupils' family members ☐ External organisations ☐ Members of the public ☐ Others: *please provide details*	
PROPOSED CONTRIBUTORS **Please tick all that apply.**	
☐ Students of Fulham School (specify age range) ☐ Fulham School staff ☐ Students' family members ☐ External organisations	

□ Members of the public □ Others: *please provide details*

ADMINISTRATION	
Names of administrators *(The site must have at least two approved administrators)*	
Names of moderators *(The site must have at least two approved moderators)*	
Who will host the site?	□ Fulham School □ Third Party Host Name:_____
Proposed live date:	
Proposed closure date:	
How do you propose to advertise for external contributors?	
If contributors include children or adults with learning disabilities how do you propose to inform and obtain consent of parents or responsible adults?	
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' of the site?	

APPROVAL		
Line Manager I approve the aims and content of the proposed site.	Name: Signature: Date:	
IT Manager I approve the aims and content of the proposed site.	Name: Signature: Date:	
Head I approve the aims and content of the proposed site.	Name: Signature: Date:	