CLAREMONT
FAN COURT SCHOOL

POLICY:

TECHNOLOGY ACCEPTABLE USAGE POLICY AND PROCEDURE FOR STAFF

Policy statement:

This policy applies to the use of desktop PCs, laptops, mobile phones, tablets, digital cameras and any other similar devices and applies to all members of the school staff community who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

At Claremont Fan Court School we believe that computers are essential tools used to support learning and teaching. We also recognise that other electronic devices such as mobile phones and tablets play an increasingly important role in the life of the pupil. With these tools comes a responsibility that must be accepted by our school community. Our school network provides access to shared resources such as printing, file storage, email and the internet, which offers vast, diverse, and unique educational resources. This worldwide access is accompanied by additional responsibilities. The users' behaviours and actions now represent the Claremont Fan Court School community in a global arena.

The ICLT provision, including laptops, provides a positive impact for learning and administration and is at the core of school operations. Staff who use school laptops, desktop PCs or other electronic devices understand and accept that it is school owned and the following guidelines must be adhered to. Breaches of these guidelines may result in disciplinary proceedings and/or notifying the appropriate law enforcement agency.

1. Computer technology and internet safety

The following paragraphs refer to the use of all school desktop PCs, laptops and any other electronic devices owned by or brought into school by staff.

The following uses of the Claremont Fan Court School network and internet access are NOT permitted:

1. Accessing, uploading, downloading, or distributing pornographic, sexually explicit, extremist, terrorist or otherwise obscene material or material of an excessively violent or hateful nature. If a suspected criminal act has been committed, the school is legally required to contact the police.
2. Transmitting obscene, abusive, or sexually explicit language.

3. Accessing another person's information without their permission.
4. Violating copyright or otherwise using the intellectual property of another individual or organisation without permission.
5. Attempting to circumvent network filters or security systems.
6. Identifying yourself as someone other than who you are.
7. Using the network or accessing the internet for financial gain or commercial activity.
8. Using the network or accessing the internet for dating purposes or gambling.
9. Installing any software onto a device connected to the school network without permission from a member of the ICLT department.
10. Personal electronic devices will only be connected to the school network with permission from the ICLT department.
11. The use of social networks or applications such as Facebook or Instagram are not permitted on the school's network during working hours other than through the school's authorised accounts.

The following rules of technology usage, security and personal responsibility are to be observed at all times:

1. Adhere to the same standards of behaviour online that you expect offline. Be polite. Abusive, derogatory language or cyber-bullying is not permitted or tolerated.
2. All electronic communications with pupils, parents and other professionals will only take place via a school email address and communication must be in a professional manner at all times.
3. Laptops, electronic devices and desktop PCs must be screen locked or logged off when the users are away from the device.
4. All confidential staff or pupil data saved to the laptop must be password protected and removed from the laptop when no longer required.
5. Any confidential staff or pupil data that needs to be shared with external parties must be password protected before sending. Files should be placed in secure areas within Teams when sharing confidential data amongst staff.
6. Staff and pupil personal data must be treated securely, confidentially and with privacy and respect, and used only for legitimate and reasonable school business purposes. No personal data should be shared with any external organisation without ensuring they are compliant with current data protection laws and there is a school business case to do this. Any data breach will be considered a contravention of current data protection laws and may result in disciplinary action and the breach being reported to the Information Commissioner's Office.
7. Staff must not save or store any pupil or staff sensitive or confidential data to any removable or personal device such as, but not limited to: USB sticks, CDs, DVDs, external hard drives, personal mobile phones and cameras, or personal online storage facility such as, but not limited to "Dropbox" and "Google Drive". School-managed storage accounts, eg MS Teams is permitted to store such data as long as appropriate permissions are set to protect the data.
8. The laptop or other electronic device may be used for personal use, provided such use is totally acceptable in a school situation. The laptop should have no

material or wording saved onto it that would not be appropriate for any other member of the school community to view.

9. Social networking sites are public spaces and the same level of professional, ethical and moral behaviour is expected from staff as that required in any aspect of their public life. Actions that damage the reputation of the school may lead to disciplinary measures.
10. Staff members who access the school email or network via the use of personal devices will be expected to adhere to the same levels of data protection as those using school issued laptops or desktop PCs.
11. Staff who have access to the school network via an external VPN link must follow the two-factor authentication log in process and ensure they log out immediately after use.
12. Staff must not disclose or write down any password or security information. Staff must use a ‘strong’ password (a strong password contains a combination of numbers, letters and symbols, with 8 or more characters).
13. No pupil is allowed to log on to any device, network or online service using a teacher’s account. Staff devices may not be used by anyone who is not a member of staff (note this exclusion includes family members)
14. Laptops must be locked when left unattended.
15. Damaged or faulty laptops, chargers or other devices must be reported to the ICLT department immediately and not used as they could be potentially hazardous.
16. If a laptop or a school provided electronic device goes missing or theft is suspected, the member of staff must report this to the ICLT department immediately as this may need to be reported as a data breach to the Information Commissioner's Office.
17. The laptop or other electronic device must be kept in a safe place when not being used. It must never be left where persons not entitled to view this information may gain access to it.
18. If a member of staff is on a long-term absence, which requires the school to employ a substitute, the laptop must be returned for the period of substitution, unless by prior arrangement with the head of school.

Filtering and Monitoring and keeping the school network safe

The school has appropriate filters and monitoring systems (Smoothwall) in place to safeguard pupils and staff from potentially harmful and inappropriate material online when using the school's IT system. Certain categories of websites are blocked by the school's filtering system and the ICLT department and designated safeguarding lead monitor email and internet traffic for both staff and pupils.

The school ensures compliance with the DfE’s ‘filtering and monitoring standards for schools’ by;

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing the filtering and monitoring provision at least annually

- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet our safeguarding needs.

- In terms of filtering, the school utilises a firewall service (Smoothwall) to filter content and thus ensure that all pupils and staff using the CFCS Wi-Fi are prevented from being able to access or receive material that is not suitable for a place of education and/or work. For devices issued or managed by the school (including all staff laptops) this filtering operates whether the devices are on or off the school premises.

- In monitoring terms, CFCS uses the Smoothwall platform including the full monitoring service (FMS), to ensure that pupil devices are monitored 24/7 (including when off-site) for any inappropriate and/or concerning use of language and/or attempts to access content which is inappropriate (balanced alongside access for educational need). Smoothwall monitoring and safeguarding software triages alerts according to their severity, which includes an email alert service at 'L4' and a phone call to the DSL for 'L5'. Finally, CFCS makes use of Sophos as an Internet security software (like anti-virus) which blocks bad applications and this is monitored by the IT team. The DSL is ultimately responsible for all elements of the above and meets regularly with the ICLT department to ensure the systems are working as expected. These systems are reviewed on an annual basis.

- Upon request of the senior leadership team a staff member must provide access to their laptop or school owned device. The school reserves the right to review any information stored on a staff member's laptop including any removable media they may have with them at school. This will only be requested when a suspected aspect of the technology acceptable usage policy has been violated. At all other times we respect an individual's right to keep their data confidential in accordance with current data protection laws. Violations by staff will be recorded and may be used to support disciplinary action or criminal proceedings.

2. Taking, storing and using images (photographs and videos) of children

Claremont Fan Court is an open and inclusive community that is very proud of its pupils in their academic, artistic and sporting achievements. The school is decorated with examples of pupils′ work, team photographs and photographic records of trips and expeditions. The school′s website and authorised social media accounts are updated regularly and parents receive newsletters with news of school activities.

Any member of staff responsible for managing official school social media accounts must ensure they have read, understood and signed to indicate their adherence to the school's social media policy.

Data protection laws and how they apply to taking, using and storing images of children

Claremont Fan Court staff can use photographic images of its pupils (unless a parent has refused consent) for the following purposes:

1. Internal displays on digital and conventional noticeboards within the school premises.
2. Communications with the school community (parents, pupils, staff, Governors and alumni) via the school's official platforms such as newsletters, the school's website and authorised social media accounts. Note: first name only should be used in external communications.
3. Marketing the school digitally through the website, the school prospectus, local press, displays at educational fairs and other marketing functions within the UK.

Images that the school uses in displays and on its website

The following guidelines must be adhered to when using images for displays and communications purposes:

1. Images must never identify an individual pupil by their full name or other personal information.
2. Staff must only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context.
3. Staff must never use any image that might embarrass or humiliate a pupil or where pupils are not suitably dressed.
4. Pupils must always be properly supervised when professional photographers visit the school.

Use of cameras and recording equipment and pupil images by staff including EYFS

The following guidelines must be adhered to when using cameras, recording equipment and pupil images:

1. Images should only be taken and edited on school issued equipment and not on staff personal cameras, phones or other devices. In an unavoidable situation where a staff member has used their personal device, the image must be downloaded to the school network at the earliest opportunity and deleted from their personal device.
2. Staff members should be sensitive to any pupils who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.
3. All photographs taken of pupils should have context. Staff should avoid one-to-one situations with no surrounding context.
4. All pupils must be appropriately dressed.
5. The use of cameras is prohibited in toilets and changing areas (including backstage).
6. All images will be stored securely and used only by those authorised to do so. All images not retained for further use must be deleted.
7. No images must be made for personal use and if questioned, a staff member must be able to justify any image of a pupil found in their possession.

8. Staff are prohibited from using any pupil images on any external website or platform other than its own official school platforms.
9. When using MS Teams or Google Meet, or other similar video conferencing software or platform staff must record any meetings with students.

Use of images for internal identification

All staff and pupils are photographed on entering the school and, thereafter annually, for the purpose of internal identification. Imagery Is securely stored in the school database where access is restricted to academic, pastoral and administrative staff.

CCTV

Claremont Fan Court believes that closed circuit television cameras (CCTV) offers improved security protection for both pupils and staff. Claremont Fan Court School informs parents and staff that it has CCTV installed on its premises for the sole purpose of surveillance for security reasons. Notices are clearly displayed in areas around the school. It is not installed in changing rooms or toilets.

Claremont Fan Court is registered with the Information Commissioner's Office and has an appointed member of the school's management team who oversees all aspects of the use of surveillance CCTV within the school. Parents are assured that Claremont Fan Court does not stream images collected via CCTV to any third parties or outside agencies. Please note that the school may be legally required to provide CCTV footage to the police or other law enforcement agencies if requested.

Treating others with respect

Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. In accordance with our mission and values, Claremont Fan Court is strongly committed to promoting equal opportunities for all.

It is reasonable to accept that some staff and parents will send email correspondence outside the school day, ie during the evening or at weekends. The school does not expect the recipient to respond until the following school working day, unless the matter is urgent. The emailing of pupils in the evening or at weekends is discouraged unless it is an urgent matter which cannot wait until the next school day.

All staff and pupils are encouraged to look after each other and to report any concerns about the misuse of technology or a worrying issue to their line manager or member of the senior leadership team. The misuse of technology will always be taken seriously and may be the subject of disciplinary procedures.