Newham Collegiate Sixth Form Centre

A specialist centre for Science and Mathematics

ICT USAGE POLICY

Written by: Joanne Spiller
Date: 1st December 2018
Approved date: 3rd December 2018
Review date: No later than December 2020

Introduction

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of young people and adults. Information and Communications Technology covers a wide range of resources including; web---based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society and within the Sixth Form context. Currently the information technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial, ICT and web---based resources need to be carefully managed. All users need to be aware of the range of risks associated with the use of these technologies. At NCS we understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain safe and within the law when using the internet and related technologies, in and beyond the context of the classroom.

Everybody in the Sixth Form has a shared responsibility to secure any sensitive information used in their day to day professional duties and should be made aware of the risks and threats and how to minimise them. This policy applies to fixed and mobile internet technologies provided by the Sixth Form (such as PCs, laptops, IPads, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto Sixth Form premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

This policy applies to full---time and part---time employees of the Sixth Form, beginning teachers and other staff on placement working at the Sixth Form in whatever capacity.

Staff, Governors and Other Authorised Users

The Sixth Form has installed computers, issued laptops and provided Ipads with internet access to enhance learning and teaching. Like all other Sixth Form equipment, the hardware / software and computer network should be treated with respect. The computer system is owned by the Sixth

Form. Staff may use it to enhance their professional activities, including teaching, research, administration and management.

All Staff must

- Ensure that virus checking facilities are used on laptops and report immediately any incidence of viruses to the ICT technicians
- Only use authorised, licensed software
- Ensure that copyright of materials is respected;
- Ensure that all internet usage should be appropriate to staff professional activity or the student's education;
- Only access your authorised account via your password, which should not be made available to any other person;
- Not do any activity that threatens the integrity of the Sixth Form ICT systems, or activity that attacks or corrupts other systems;
- Be responsible for all email sent and for contacts made that may result in email being received;
- Report any unpleasant material or messages sent;
- Not post anonymous messages or forward chain letters and emails;
- Ensure that as email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should apply as for letters or other media;
- Use all equipment economically, including printers.
- Staff must not knowingly access, view, download, upload, record, retain, disseminate, display or otherwise process any image, text, data, sounds, material and software which:
  a) May be considered offensive or abusive (for example where the content may be considered to be racist, sexist, profane or a personal attack)
  b) May be considered to be obscene, indecent or otherwise pornographic.
  c) Will be used for personal financial gain, gambling, political purposes or advertising.
  d) Encourages or promotes activities which may be illegal or unlawful such as the use of pirate and/or illegally copied software

The Sixth Form reserves the right to examine, check or delete any files that may be held on its computer system or to monitor any internet sites visited. **Staff who violate any of the above rules risk disciplinary action and, if applicable, external agencies may be involved.**

Expectations of ICT Network Support Staff

When required to, for the purposes of carrying out their job, the Network Manager, with permission from the Principal, may:

- Authorise the Installation of software for testing and other purposes
- Log on as other users

- Change user passwords and other account details
- Inspect users accounts and documents
- Access administrative tools
- Test network security
- View material otherwise considered inappropriate whilst investigating incidents
- View staff and student activity through access logs and monitoring tools.
- Such exceptions to the general policy should be authorised by the Network Manager and Principal (or designated representative) and recorded. Where investigation is required into a suspected breach of the code of conduct, by a user, at least two members of staff (usually a member of SLT and the Network manager) should jointly conduct the investigation.
- Any safeguarding issues that arise from such investigation should be referred to the Sixth Form's Safeguarding Officers.

Monitoring

The Principal may monitor, intercept, access, inspect, record and disclose emails, instant messaging, internet/intranet use and any other electronic communications (data, or image) involving employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain Sixth Form business related information; to confirm or investigate compliance with Sixth Form policies, standards and procedures; to ensure the effective operation of Sixth Form ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

All monitoring, surveillance or investigative activities are conducted by authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.
Please note that personal communications using Sixth Form ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

A breach or suspected breach of policy by a Sixth Form employee, contractor or student may result in the temporary or permanent withdrawal of Sixth Form ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the Sixth Form Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings. The Information Commissioner's Office (ICO) new powers to issue monetary penalties came into force on 6 April 2010, allowing the ICOs to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

Incident Reporting

Any security breaches, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Network Manager. Additionally, all security breaches,

lost/stolen equipment or data (including remote access), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported at the first opportunity.

The use of email is an essential means of communication for both staff and students. In the context of Sixth Form, email should not be considered private.

The Sixth Form gives all staff their own e---mail account to use for all Sixth Form business as a work-based tool. This is to minimize the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. The Sixth Form email account should be the account that is used for all Sixth Form business.

Under no circumstances should staff contact students, parents or conduct any Sixth Form business using personal email addresses

Although personal use of email facilities is discouraged, limited personal use will be permitted provided that the content of messages is appropriate, i.e. is not likely to cause offence. Employees should regard this facility as a privilege that should be exercised in their own time without detriment to the job and not abused. Inappropriate or excessive use may result in disciplinary action and/or removal of facilities. However, staff should be aware that both private and business use of email will be subject to monitoring by the Principal.

Confidentiality can be compromised, especially when using internet based email systems. Employees should, therefore, not send legally confidential information via the internet unless the data is encrypted. The internal email system is however sufficiently secured for internal communication but care should be taken.

Email – dos and don'ts at NCS

- Do not send to "ALL STAFF" unless it is absolutely necessary. Find the relevant people required for your message before sending.
- Do not send messages pertaining to student's lost property. All enquiries of this nature should be directed to the Sixth Form office.
- If a student is absent from your lesson and it is not listed in the students out system please send an ALL STAFF and OFFICEADMIN email to see if the student's location is known. This is to protect the health and safety of all students.
- Do not use aggressive or abusive language or tones in Emails. (Using capital letters to reinforce a point may be deemed aggressive and is unnecessary).
- Do not use email to have a difficult conversation or to address a sensitive/difficult issue. Arrange a time to meet the person on a face to face basis.

Legal Contract and Freedom of Information Act Concerning Email

Email is capable of forming or varying a contract in just the same way as a written letter. Such capability gives rise to the danger of employees inadvertently forming contracts on behalf the Sixth Form or varying contractual terms to which the Sixth Form then becomes bound. For the avoidance of doubt, employees cannot form legally binding contracts on behalf of the Sixth From without prior written approval from the Principle. Employees should take due care when drafting the words of an email so that they cannot be construed as forming or varying a contract when this is not the intention. The freedom of information act essentially states that any email can be used as evidence in a legal case. **Staff must therefore be aware that any communication they send, receive or even forward can be used as a legal document as evidence in a court of law.**

Internet Access

The internet is an open communication medium, available to all, 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. All use of computers/Ipads at NCS is monitored. Logs are made and checked randomly but regularly. Whenever any inappropriate use is detected it will be followed up.

If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research. All users must observe copyright of software and other materials at all times. It is illegal to copy or distribute Sixth Form software or illegal software from other sources.

Internet Use

- You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Don't reveal names of colleagues, customers or clients or any other confidential. information acquired through your job on any social networking site or blog
- Online gambling or gaming is strictly prohibited.

Social Networking and Online Conduct

It is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism concerning social networking. To this end, we require our staff and students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

Purpose

The purpose of this policy is to ensure:

- Staff and students are kept safe online and are not exposed to potential risks.
- That members of staff are fully aware of the potential risks associated with the use of social media and the rules governing its use
- That members of staff work with students to promote the safe use of social media
- That the Sixth Form and Local Authority are not exposed to legal risks
- That the reputation of the Sixth Form is not adversely affected
- That stakeholders and those from the wider community are able to clearly distinguish where information provided via social networking applications is legitimately representative of the Sixth Form

Scope

This policy covers the use of social networking applications by all Sixth Form stakeholders, including, employees, governors and students. The requirements of this policy apply to all

uses of social networking applications which are used for personal or Sixth Form related purposes.

Social networking and online applications include, but are not limited to:

- Blogs and weblogs, for example Blogger, Wordpress etc.
- Online discussion forums of all kinds e.g. mumsnet. This includes comment sections on newspaper website
- Collaborative spaces, such as Facebook, Media sharing services, for example YouTube, Flickr, Photobucket, Instagram
- 'Micro---blogging' applications, for example Twitter
- Cloud file storage and sharing such as Office 365, ICloud and Dropbox.

For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, IPad, cameras or other handheld devices and any other emerging forms of communications technologies.

All Sixth Form representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the Sixth Form's Equality and Diversity Policy.

Guidance for Staff

Terms of Use

Communication with students

- No member of staff should interact with any student in the Sixth Form on social networking sites. For example this includes becoming a 'friend' on Facebook or 'following' a student on Twitter. Staff should employ the highest possible security settings on their accounts and scrutinize any new 'followers' and 'friends' to ensure no improper interaction.
- No member of staff should interact with any ex-student in the Sixth Form on social networking sites who is under the age of 18.
- Where family and friends have students in Sixth Form and there are legitimate family links, please inform the Principal in writing. However, it would not be appropriate to network during the working day on Sixth Form equipment.
- No member of the Sixth Form staff should request access to a student's account on the social networking site. Neither should he/she permit the student access to the staff members' area e.g. by accepting them as a friend.
- Staff may only create blogs, Wikis or other platforms in order to communicate with students after it has been approved in writing by the Principal.

- If administering or contributing to approve Social Media for work purposes, staff will be required to create an account for this purpose, e.g. twitter handle or Gmail, so as to separate personal from professional communication. This will involve using their NCS email and Sixth Form picture.
- All posts and comments on these approved forms of social media should represent the Sixth Form professionally and as such may be monitored by the Sixth Form in the same way as email.
- It is illegal for an adult to network by giving their age and status as a child.

Communication in the Public Domain

1.Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, students or other individuals connected with the Sixth Form, or another Sixth Form, or CoLAT could result in formal action being taken against them.

2.Members of staff are also reminded that they must comply with the requirements of equalities legislation in their online communications.

3.Members of staff must never post derogatory remarks or offensive comments online or engage in online activities which may bring the Sixth Form or CoLAT into disrepute.

4.Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct.

5.CoLAT expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these terms of use.

6.Colleagues must also be aware of copyright issues when sharing resources through Social Media e.g. Google+. As such there can be no sharing of resources which are not wholly created by the individual teacher.

7.Furthermore no Sixth Form owned material, policies or resources are to be shared in the public domain without the written permission of the Principal.

8.Please note legal guidance on sharing resources that you may have created yourself publicly. “If a piece of work is original and eligible for copyright, the employer automatically owns anything created by employees during the normal course of their duties”. Please discuss with SLT member in charge of ICT if necessary.

9.Staff may only create blogs, Wikis or other platforms in order to communicate with colleagues, both in Sixth Form and globally, after it has been approved by the Principal.

10.If administering or contributing to approved Social Media, staff will be required to create a new account for this purpose, e.g. Twitter handle or Gmail, so as to separate personal from professional communication. This will involve using their NCS email and Sixth Form picture.

11.All posts and comments on these approved forms of social media should represent the Sixth Form professionally and as such may be monitored by the Sixth Form in the same way as email.

Protection of Personal Information

1.Staff should keep their personal phone numbers private and not use their own mobile phones to contact students or parents.

2.Some social sites and other web---based sites have fields in the user profile for job title etc. If you are an employee of a Sixth Form and particularly if you are a teacher,

3.We recommend that you should not put any information onto the site that could identify either your profession or the Sixth Form where you work. In some circumstances this could damage the reputation of the Sixth Form, the profession or the local authority. If you choose to include this information on your public profile(s) then be aware that you may be exposed to more risks as outlined in this document.

4.Staff should not join NCS related groups, both official and unofficial, with their personal accounts. For example joining an NCS Facebook group.

6.Staff should never share their work logins or passwords with other people.

7.Staff should never give their personal email addresses to students or parents. Where there is a need for home learning to be sent electronically the Sixth Form email address should be used.

Related Issues

1.Staff should not take photos or record videos in work time using unapproved or personal devices.

2.Staff must only use approved tools for recording activities in work time e.g. Sixth Form IPod or IPad.

3.Photos or videos taken in Sixth Form time are not to be posted to any social network without written permission from the Principal.

Raising Concerns

If you have any evidence of students or adults using social networking sites in a manner which is not in accordance with the above guidance then please contact the named child protection person in Sixth Form in accordance with our Safeguarding Policy.

Guidance for Students

1.Students will not have access to any social networking site via the Sixth Form network.
2.Students in the Sixth Form are allowed to access mobile phones in designated areas and as such will make use of Social Media.
3.All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
4.Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
5.Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, Sixth Form details, IM/ email address).
6.Students are encouraged to be wary about publishing specific and detailed private thoughts online.
7.Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
8.The Sixth Form will update and maintain guidance for students to ensure their E-safety.

Enforcement

1.Social Media, email or text communications between an adult and a student outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites. Internal e---mail systems should only be used in accordance with the Sixth Form's policy.

2.Any breach of the terms set out could result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible Sixth Form representative being suspended.

3.CoLAT reserves the right to require the closure of any applications or removal of content published by Sixth Form representatives which may adversely affect the reputation of the Sixth Form or put it at risk of legal action.
4.Any communications or content you publish that causes damage to the Sixth Form, Local Authority, any of its employees, students or any third party's reputation may amount to misconduct or gross misconduct to which the Sixth Form and Local Authority Dismissal and Disciplinary Policies apply.