CAMBRIDGE CENTRE FOR SIXTH-FORM STUDIES

IT ACCEPTABLE USE POLICY

Guidance for Staff and Pupils

Contents

1. Scope

This policy (the **"Policy"**) applies to users (professional and support staff, students and others with access privileges) of all IT facilities and other learning resources owned or otherwise used or provided by Cambridge Centre for Sixth-form Studies (**"CCSS"**) at each of its teaching and boarding sites (the **"IT Facilities"**). This includes all IT equipment connected to CCSS's servers or network.

The Policy is under regular review and may be changed from to time and users are therefore required to refer to the on-line version of the Policy on CCSS's SharePoint site.

Staff and students should note the consequences of failing to comply with the Policy which are set out in paragraph 6 below.

If you have any queries on the Policy, please contact: The Deputy Principal.

2. Use of IT Facilities

General

Use of the IT Facilities constitutes acceptance of the Policy and users must comply with all applicable laws.

Users must respect the rights, privacy and property of others and use the IT Facilities for the purpose for which they are intended, namely to support the teaching, learning, research and administrative activities of CCSS. Users must conduct themselves accordingly when using the IT Facilities to create a beneficial environment for all and must not interfere with or disrupt the availability or use of the IT Facilities by others.

Each user will be issued with a username and password. Passwords must not be disclosed to anyone and any temporary passwords must be changed immediately following a successful login. Staff members must not allow a student to use their login details to use the IT Facilities.

Where CSSS's network is used to access other networks, any abuses against those other networks will be regarded as an unacceptable use of CCSS's network.

Personal Use

Limited personal use of certain IT Facilities is permitted during personal time. Any such use must neither interfere with the work of the employee or the study of the student nor prevent others from carrying out their legitimate work and use of the IT Facilities. CCSS reserves the right to withdraw this benefit either individually or collectively at any time.

Commercial Use

Use of any of the IT Facilities for commercial gain (including advertising) or for work on behalf of others (unconnected with a student's course of study at CCSS or a member of staff's legitimate activities) is prohibited unless the user has the prior written consent of The Deputy Principal.

Movement

The IT Facilities, with the exception of portable computers, should not be moved or disconnected.

Damage

Users must not cause any damage to the IT Facilities or any of the rooms and their facilities and services which contain the IT Facilities (which includes the unauthorised installation of hardware or software). Under no circumstances must food or drink be consumed near any of the IT Facilities.

Spam and Mass-circulation

Spam is usually defined as unsolicited electronic messages (using email, SMS, Instant Messaging or other means) sent in bulk. Users may not use the IT Facilities to send spam.

All effort is made to filter out incoming spam before reaching users' inboxes but this is not guaranteed and the occasional message may reach a user.

Security

Users must not deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into the IT Facilities, nor take deliberate action to circumvent any precautions taken by CCSS to prevent this. Users must not attempt to penetrate the security and/or privacy of other users. All of the IT facilities have anti-virus and anti-spyware protection installed. Any personal devises connected to the network must have anti-virus installed with up to date virus definitions.

Illegal and/or Offensive Material

Users must not use the IT Facilities to access, produce, obtain, download, store, view, share or distribute material (including images, video, text or sound files) which is either illegal under UK law and/or can be reasonably judged to be offensive, likely to incite racial hatred, obscene, indecent or abusive. The only exceptions would be where such material is essential for research or teaching and is permitted by law and prior permission has been given by The Deputy Principal.

Discrimination

Users must not use the IT Facilities to place, disseminate or receive materials which discriminate or encourage discrimination including on the grounds of gender, sexual orientation, religious belief, disability, age, race or ethnic origin.

Defamation

Users must not use the IT Facilities to publish any information which they know or believe to be untrue or is defamatory and could not be defended on the grounds that it is true/factual.

Cyber-bullying

The advent of cyber bullying adds new dimensions to the problem of bullying. Cyber bullying can follow students into their private spaces and outside school hours. CCSS issues guidance to students through the student/parent handbook and via tutors provides guidelines on where to go for help. CCSS reserves the right to monitor students' use of the internet on a routine basis and to examine mobile phones where there is a reason to suspect abuse. Students are held responsible for all material they place on a website and for all material that appears on a

website of which they are the account holder. CCSS promotes the positive use of new technologies through its policies, curriculum delivery, pastoral tutorials and PSHE.

CCSS regards cyber-bullying through inappropriate use of electronic communications such as text messages, email or postings on social networking websites as unacceptable.

Social Networking

The popularity of social media sites such as Facebook, YouTube, Twitter, LinkedIn, and others, grows constantly. CCSS's policy can be summarised in one sentence: "Be cautious, exercise good judgement and use common sense."

Whether or not a member of staff or a student chooses to participate in online social media, it is his or her own decision. However, to the extent that staff, students and other members of CCSS community represent CCSS on the internet, participation in social media should be done responsibly, with a mind towards how both the location where one chooses to participate and the content one posts reflect on that person and on CCSS.

Everything you contribute online stays online forever in some format and everything you do, often on a personal basis, reflects on CCSS as an organisation. Ask yourself: "Would it make my colleagues, other teachers or students uncomfortable? Would this public expression impair my ability to work with my colleagues/fellow students on a friendly basis? Would it give an advantage to our competition? Could it damage the reputation of CCSS?"

While open communication both internally and externally in all forms is encouraged, we expect and insist that such communication does not substantively demean our environment. This means that constructive criticism is welcome where appropriate, both privately and publicly, but harsh or continuous disparagement is frowned upon, because it is likely to be destructive and unhelpful.

Externally communicating/disseminating confidential CCSS information and/or other aspects of CCSS information that is not intended for public consumption is always forbidden and will be grounds for disciplinary measures.

Extremism and radicalisation

The use of the internet to influence those who are vulnerable to radicalisation and extremism is a serious concern on a global scale and of relevance to all in educational settings.

As with any potential hazard, CCSS uses a combination of supervision, protection and training to minimise the risk of harm. In this context, supervision is achieved largely remotely, by routine monitoring of internet access: the college reserves the right to be "looking over the shoulder" of anyone using college IT equipment or internet services.

Protection on the internet is achieved by filtering access, which CCSS does minimally because of the degradation of legitimate service that this causes. The college instead monitors traffic to check for any warning signs of potential misuse.

All students have access in Cambridge to fast 3g or 4g services on their own mobile devices that render any efforts by the college at supervision or protection completely ineffective. Our most effective means of protecting students is therefore the training that we provide by the nature and content of the education at CCSS. Championing individual liberties, respect for the views of others, and mature discrimination about ideas and ideologies are just some of the characteristics that are encouraged in our students.

As with the approach to cyber-bullying, CCSS promotes the positive use of new technologies through its policies, curriculum delivery, pastoral tutorials and PSHE.

Users should therefore be aware that CCSS reserves the right to monitor any or all activity on its system, and reserves the absolute right to immediately suspend, dismiss or expel (as appropriate) any individual found to be in breach of any of the policies relating to Extremism, Security, Illegal and/or Offensive Material, Discrimination, Defamation, Cyber-bullying and/or Social Networking.

3. Monitoring of IT Facilities

It will and log files, messages, emails and user account information may be intercepted, monitored, recorded, copied, audited and inspected.

The IT department has total administrative access to all of the IT Facilities and has the right to monitor and access all IT Facilities including any saved files. Any misuse of the IT Facilities found by the IT department will be reported to The Deputy Principal.

Confidentiality

Absolute confidentiality cannot be guaranteed.

Any emails or files, stored and/or sent or received may be accessed by individuals other than the individual for whom it was intended, whether by accident (eg. a computer left logged on) or design (eg. an email may need to be opened to diagnose connectivity problems which have been brought to the attention of the IT department).

In the case of external (internet) email, these can potentially be intercepted and read by third parties without CCSS's knowledge.

Messages of particular confidentiality or sensitivity should be sent by an alternative medium.

Internet Access

Internet access is provided for educational, administrative, research and personal development use. Internet users do not have a right to confidentiality or privacy when using or accessing the IT Facilities. CCSS uses monitoring software to monitor content. Misuse or visits to sites of an improper nature will automatically be reported to The Deputy Principal. Summary activity reports will be generated and reviewed twice each month to monitor inappropriate use.

Emails and Files

CCSS reserves the right to retrieve the contents of messages and files for the following purposes:

- to monitor whether the use of the email system/storage medium is legitimate and in accordance with the Policy;
- to find lost messages/deleted files or to retrieve messages/files lost due to computer failure;
- to assist in the investigation of wrongful acts;
- to comply with any legal obligation.

Monitoring will only be carried out to the extent permitted or required by law. CCSS will not routinely monitor email messages/files. Spot checks or tailored searches may be done in the

context of disciplinary proceedings (whether actual or contemplated) or where CCSS has reason to believe that the systems may be being used in breach of the Policy.

Software

Student users of the IT Facilities are not authorised to load any software onto the IT Facilities. It is forbidden, under any circumstances:

- to run peer to peer (P2P) software such as Kazaa, eDonkey, Bit Torrent or Limewire on any of the IT Facilities; and
- to download software from the internet and/or software obtained illegally onto the IT Facilities.

Any breach of this policy will be reported to The Deputy Principal.

4. Maintenance & Repairs

Maintenance is controlled by the IT department in conjunction with external suppliers. Any faulty/out of order IT Facility should be reported to the IT department as soon as the problem is found. Any data stored on faulty IT Facilities will be recovered using a 'best effort' approach by the IT department. Any cost incurred by the IT department in recovering data may be charged back to the user.

5. Copyright and Licence Agreements

Users must adhere to the terms and conditions of all licence agreements relating to IT Facilities and learning resources which they use including software, services documentation and other goods.

Users must not:

- copy or modify any copyright material (3rd party material) nor incorporate any part of 3rd party material into their own work; or
- install, make, store or transfer unlicensed copies of any copyright or trademark work including software, videos or music;

unless such acts are either permitted by law or by a licence agreement or with the permission of the copyright/trademark holder.

6. Infringement

Withdrawal of Facilities

If a user is in breach of any part of this Policy, The Deputy Principal may withdraw or restrict the user's use of the IT Facilities and learning resources following consultation with the user's head of department or in relation to students their tutor, and/or parents.

Removal of Material

CCSS reserves the right to remove material from its IT Facilities without notice where such material is in breach of these regulations.

Disciplinary Action

Any breach of this Policy may be dealt with by The Deputy Principal under CCSS's formal disciplinary procedure for both students and staff and in some cases may result in suspension,

expulsion or dismissal. The user may be charged for any costs that have arisen as a result of misuse or abuse of the IT Facilities and/or learning resources.

Breaches of Law

Where appropriate, suspected breaches of the law may be reported to the police. Where the breach has occurred in a jurisdiction outside the UK, the breach may be reported to the relevant authorities within that jurisdiction.

7. Disclaimer

CCSS accepts no responsibility and expressly excludes liability to the fullest extent permissible by law for:

- the malfunctioning of any IT Facility or part thereof, whether hardware, software or other;
- the loss of any data or software or the failure of any security or privacy mechanism.

Reviewed September 2016