The ContinU Plus Academy

2021-22

Acceptable Use of Electronic Communications Policy

The ContinU Plus Academy Acceptable Use of Electronic Communications Policy (including ICT Network Use & Data)

1. Introduction

The Acceptable Use of Electronic Communications Policy applies to members of staff or contract staff that are employed by the ContinU Plus Academy (CPA) and who need to access the ICT Network. The Acceptable Use of Electronic Communications Policy also applies to CPA owned equipment which is not connected to the network.

Responsibility for updates and the maintenance of the Acceptable Use of Electronic Communications Policy rests with the CPA's Business Manager.

Policy Statement:

The CPA provides PC's, laptops and tablets as well as access to e-mail and the Internet. The CPA encourages their use wherever it assists job performance. The Acceptable Use of Electronic Communications Policy applies to all users of the CPA's PCs, laptops and tablets as well as everyone who has access to the CPA's network, including employees, agency staff or contractors. This policy applies to the school's ICT systems, hardware and software, also to the 'words' whether spoken or transmitted electronically via e-mail and content transmitted across any such system.

The CPA has a number of legislative requirements that must be adhered to in relation to the IT network and any specific applications, e-mail and Internet use. The Acceptable Use of Electronic Communications Policy defines for all staff what is acceptable and unacceptable use of the CPA's systems.

The Acceptable Use of Electronic Communications Policy is important to make staff fully aware of what constitutes misuse.

This Acceptable Use of Electronic Communications Policy supersedes all others and applies to staff only.

2. Risks to the School & Legal Requirements

2.1 Risks to the School:

Whilst use of e-mail and the Internet in particular is often essential for job performance, it can expose staff and the CPA to the risk of a legal claim including:

- a defamation claim;
- a discrimination claim, whether on the grounds of gender, race, disability, sexual orientation, religion or age;
- a harassment or use of offensive language claim;
- a breach of copyright claim;
- a breach of contract claim;
- a claim for breach of the duty of confidentiality;
- a criminal prosecution following the discovery of child pornography or unlicensed software (such as books, films or music) on the network;
- a criminal prosecution or civil action following a breach of data protection legislation.

It is for this reason that the CPA needs to set out in this policy clear rules for use of its systems, the consequences of misuse and the measures the school will take to monitor compliance with the policy.

Guiding Principle:

If staff are in any way unsure or unclear whether their use of the school's ICT facilities and equipment could be deemed as inappropriate or likely to lead to a claim of misconduct they should discuss their concerns with their line manager or SLT before using the system.

2.2 Legal Requirements:

The following legal requirements have been considered in the formation of this policy.

Data Protection Act 2018	Messages containing personal information, personal opinions about an individual or the opinions of an individual are all covered under the Act. Advice suggests that the risk of not monitoring illegal content, time wasting by employees, breach of copyright and defamation outweighs the entitlement to privacy under the Human Rights Act. In order to comply with the law, any monitoring that is undertaken must follow the procedures outlined in the policy.
Human Rights Act 1998	Under article 8 of the Human Rights Act 'everyone has a right to respect for his private and family life, his home and his correspondence'.

Freedom of Information Act 2000	All e-mails fall within the scope of the Act.
Regulation of Investigatory Powers Act 2000 & the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000	All interception must be authorised and there must be mutual consent and good business reason for doing so. Includes access to e-mails before they have been opened by the intended recipient however does not include items opened and stored.
Defamation Act 1996	E-mail can contain defamation and it circulates very quickly, because of the broadcasting capabilities of e-mail, defamatory comments are likely to be treated as libel and therefore there is no requirement to prove damage.

3. Use of School ICT Systems

At all times users must comply with the law in their use of the CPA's ICT equipment and systems. Examples of inappropriate activities includes, however is not limited to, examples quoted in this section of the policy.

3.1 IT Network & Applications:

The CPA is at risk from virus attack and loss of reputation caused by unprofessional work practices. To minimise these threats users should not:

- install or download non-business related software (ICT Support can advise staff on this);
- connect a PC or laptop which is not CPA property and which has not been already connected to the network by ICT Support;
- store data about individuals on the system unless the storage is covered by the CPA's data protection registration under the Data Protection Act 2018;
- fail to comply with the CPA Password Use Policy (for example allowing another user access to their password or leaving a work station unlocked);
- engage in criminal activity, for example; fraud.

3.2 Internet:

Users should not:

- visit, view or download any non job-related material from any Internet site, which contains illegal material (such as child pornography, obscene material or race hate) or other inappropriate material. Examples of inappropriate material includes, however is not limited to, criminal skills, terrorism, cults, gambling, illegal drugs and pornography.
- copy or modify copyright protected material downloaded from the Internet without authorisation;
- use the Internet for criminal activity, for example, however not limited to, software and music piracy or the sale of illegal goods;
- access unauthorised instant messaging sites of any kind.

3.3 E-mail:

Users should:

- adopt a responsible approach to the content of e-mails, bearing in mind that e-mails often need to be as formal as any other form of written correspondence such as a letter;
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion

from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

- remember that e-mail correspondence is not private as e-mails can be easily copied, forwarded or archived without the original sender's knowledge. When drafting any e-mail a user should bear in mind that it may be read by a person other than the designated recipient;
- consider whether e-mail is the most appropriate way of communicating the message, particularly when dealing with sensitive matters or where debate is likely.

Users should not:

- send an e-mail message which is abusive, malicious, discriminatory, defamatory or libellous about any person or organisation, or which contains illegal, obscene or offensive material. Before staff send or forward any e-mail they should ask themselves if they can support their actions in a disciplinary hearing or in court. It is recommended that staff inform their managers if they receive such a message;
- send e-mail which could be deemed as bullying or harassment;
- send information externally which may infringe the intellectual property rights of a person or organisation;
- open attachments or e-mails from unknown sources if they appear suspicious;
- forward 'chain mail', unsolicited bulk e-mail messages or "spam".

3.4 Personal Use:

Occasional personal usage is a privilege and can be withdrawn if abused. The CPA tolerates limited personal use of its equipment and the network provided that the following conditions are met:

- all personal usage is kept short, excessive time is not spent sending personal e-mails or surfing the Internet for non work-related purposes. The test of what is acceptable personal use is that there should be no interference with the performance of the user's work commitments or with the business use of the network. The presumption is that this activity will principally take place in the user's own time;
- That e-mail messages do not constitute misuse according to the rules outlined in this policy.

If excessive personal use is suspected then the expectation is that the line manager/SLT would speak to the individual and set more specific parameters. Line managers/SLT would be permitted to prevent all personal use if the parameters were not respected.

Users must not have an expectation of privacy when using the CPA network as all use may be monitored. If a user wishes to ensure the privacy of any information, for example when communicating with the Personnel Services or with a trade union representative, he/she should not use e-mail and instead use the post.

3.5 Disciplinary:

Breach of the regulations referred to in this section may result in disciplinary action being taken against an employee up to and including dismissal. Any action against the employee will follow the CPA's disciplinary procedures. Specific analysis of individual e-mail messages or network use will be provided in support of any investigation.

A breach of the regulations or this policy in any way by a user who is not an employee may result in legal action being taken against the user.

3.6 Password Security:

Each user gains access to the network by setting their own unique password, which must be at least eight characters long, meet certain criteria for safe passwords (mixture of upper and lower case letters, numbers and a symbol) and should be changed regularly. Best security practice is that staff should not share their password details with any other user and each user is responsible for managing their own password.

More detailed guidance can be obtained from ICT Support.

4. Monitoring & Reporting of Network Use

Monitoring describes processes that take place automatically whereby information is retained by ICT Support in order to maintain an audit trail of activity on the network. Reporting describes the extraction of data relating to individual use for the purposes of investigation.

4.1 Monitoring & Recording of Communications:

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("the Regulations") enable designated staff to carry out interception of an employee's communications using the CPA's systems for the purposes briefly described below:

- Recording the evidence of business transactions (e.g. establish facts);
- Ensuring compliance with regulatory or self-regulatory guidelines;
- Maintaining effective operation of the CPA's systems (e.g. preventing viruses);
- Monitoring standards of training and service;
- Preventing or detecting criminal activity;
- Preventing unauthorised use of the computer system - i.e. ensuring that the employee does not breach this or related school policies.

However the CPA will only do this solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the CPA's activities which pass through the CPA's own systems.

All employees should take note that every person who uses the CPA's systems to send or receive information may have their communications intercepted.

4.2 How the CPA will monitor & if necessary record?

The CPA fully appreciates that employees have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy whilst in the work environment.

Any monitoring will be carried out subject to the requirements of legislation including the Data Protection Act 1998, the Human Rights Act 1998, the Freedom of Information Act 2000, the Regulation of

Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

Network traffic and the performance of the network will be monitored and the CPA will use a firewall, anti-virus products, intrusion detection and prevention systems as well as other software to do so.

Specific monitoring of information will be undertaken as follows:

- anti-virus software will monitor all communication, however will only record and quarantine those which it identifies as containing a virus;
- software may monitor e-mail content by searching for key words. A log will be kept for 12 months of e-mails which are picked up following such monitoring;
- software will prevent access to certain designated non work-related Internet sites. A record will be maintained of sites visited and sites which users have attempted to visit;
- spot checks may be made on the communications of individuals or groups on a random basis to ensure this policy is being applied with.

The monitoring above is confined to monitoring data traffic and where appropriate recording it rather than the contents of communications. The content of communications will only be examined and reported on if it appears there may have been a breach of the law or of the CPA's policies or procedures. Personal information collected through monitoring for purposes other than those for which the monitoring was introduced will not be used unless:

a) it is clearly in the employee's interest to do so; or
b) it reveals activity that no employer could be reasonably expected to ignore.

If no further action is to be taken as a result of the report, the content will be destroyed as soon as that decision is made. If further action is taken as a result of a report then the data will be stored in accordance with the retention schedules for disciplinary matters.

4.3 Incident Reporting:

It is intended that this guidance note and associated reporting of incidents (which is set out in more detail in Appendix 1) will be used by all staff and managers who are involved in an incident or have one reported to them.

In the interests of all CPA staff they are to report all incidents of misuse with as much information as possible and for these to be investigated as thoroughly as possible.

5. Remote Use

Users will sometimes need to use CPA equipment and access the CPA network when working remotely, whether from their home, offsite or when travelling. Remote users are reminded that this Acceptable Use of Electronic Communications Policy applies to them wherever they are using CPA owned equipment and/or accessing the CPA network. Users should be particularly careful to secure access to the network by using their password when working from home, in hotels or on public transport.

Users should not:

- allow members of their family or anyone else to use the CPA network or CPA equipment;
- share or display confidential information on the screen of their computer at any time where it may be visible to a non-school employee;
- leave hardware in vulnerable locations such as cars, etc.

6. Misconduct

Compliance with the Acceptable Use of Electronic Communications Policy will be audited and for the avoidance of any doubt on the part of employees or managers, this section explains conduct or behaviour that would be deemed as 'unacceptable use'. Any breach could be deemed as serious or gross misconduct.

Examples of misconduct may include; however is not limited to:

- Sending written or verbal abusive, offensive, illegal, or defamatory messages or material;
- Sending written or verbal messages which could constitute harassment or bullying;
- Excessive personal use of e-mail or the Internet in work time;
- Introducing a virus to the system by inserting a disk or memory stick, via e-mail or from downloading an Internet file onto a CPA PC or laptop without running a virus check;
- Misuse of e-mail, the Internet or the system generally which results in a legal claim being made against the CPA;
- Accessing illegal material or pornography on the Internet;
- Unauthorised downloading of software or files;
- Accessing proxy sites or other methods to bypass systems put in place to protect the CPA network;
- Use of the Internet for criminal activity;
- Accessing other users accounts/documents and/or sharing other users information;
- Hacking or other breaches of the Computer Misuse Act 1990.

7. Safe and Responsible use of Online Social Communications

Many staff and students use the computer for social communication outside school. (e.g Facebook) Staff should not use school facilities to access or update personal social networks. Staff should be aware of the potential risk to their professional reputation of adding students, parents or friends of students as 'friends/followers' on their social network site and are strongly recommended not to do so.

Care should be taken that comments made on a social network site or blog do not relate to or identify the school, staff or pupils as this could result in disciplinary action. It is also important that photographs and descriptions of activities in the personal life of staff do not adversely affect the professional reputation of staff or the school. Staff should be aware that even if they have used the privacy settings, they may not be able to prevent material becoming public from 'friends/followers' sites.

If staff keep a personal blog the content must maintain acceptable professional standards. Any inappropriate use may lead to disciplinary action in accordance with school policy. All blogs should contain a disclaimer that the views expressed are personal and not necessarily those of the school/academy or Worcestershire Local Authority.

Schools are vulnerable to material being posted about them online and all staff should be aware of the need to report this should they become aware of anything bringing the school into disrepute. Schools should regularly check, using a search engine, to see if any such material has been posted.

Action you must take if you discover inappropriate, threatening or malicious material online concerning yourself or the school

- Secure and preserve any evidence. For example note the web address (URL), take a screen shot or copy and print the screen
- Report immediately to your line manager/SLT or head teacher
- Contact the uploader of the material or the Internet Service Provider/ site administrator and ask for the material to be removed.
  All social network sites have the means to report unacceptable material or activity on their site – some more readily available than others. If the material has been created by a pupil or staff member then the school have a responsibility to deal with it.

8. Good practice guidance for school staff

8.1 In communications with pupils and parents, never give out personal information which identifies your home address, phone number, mobile phone number or personal email address. Once such information is known you are open to harassment through unwanted phone calls, text messages and emails.

8.2 Protect your social network site by using the correct privacy settings. Make sure that personal information cannot be seen from the links to your friends'/follower's sites.

8.3 Do not accept pupils as friends/followers on your personal social network site. If at all possible do not include parents as friends/followers.

8.4 Avoid the use of chat rooms, instant messaging or other social networking services which are accessed socially by pupils and are not monitored by the school.

8.5 Always keep a copy of email communications with pupils and parents (whether sent or received) and keep a note of the dates, times and content of conversations.

8.6 If your school laptop is used outside school for non-school activities then set up a different user account to ensure that personal or confidential data is protected. Use a strong password to protect the school laptop from unauthorised access.

8.7 Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Turn it off, lock the computer, log off or set up a password-protected screen saver to prevent unauthorised access.

8.8 Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login details as you will then be held responsible for their online activity. Do not allow students to use a computer that you have logged onto.

8.9 Always use the school's digital camera or video camera for taking school related pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera's memory. Photographs of children should not be taken home to use on a personal computer.

8.10 If you are using school electronic equipment off site then take the same level of care as you would in school. A digital camera taken off site should not be returned to school with personal photographs on it.

8.11 It is not recommended that personal financial transactions are made on school equipment as information may become accessible to pupils.

8.12 Observe sensible precautions when taking photographs which may include pupils: always obtain students and/or parental permission and make sure that individual pupils cannot be identified by name, especially if the photograph is for use on the school web site. (Refer to school policy for further guidance on this issue.)

8.13 Report immediately, and in writing, to the designated person in school (or your head teacher) any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep copies as evidence.

9. General

The Acceptable Use of Electronic Communications Policy may be amended at any time and any changes will be notified to users.

Users of the CPA's network will be expected to have read and understand the Acceptable Use of Electronic Communications Policy.

Monitoring & Review

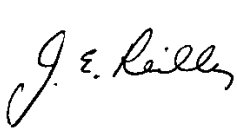
1. The impact of the Acceptable Use of Electronic Communications Policy will be reviewed by the Governing Body.
2. The Headteacher will provide the Governing Body with regular monitoring reports which will help it to evaluate the effectiveness of the Acceptable Use of Electronic Communications Policy and the procedures within.
3. The Acceptable Use of Electronic Communications Policy and its procedures will be reviewed and amended in the light of such an evaluation and in consultation with representatives of all key stakeholders.

A copy of the Acceptable use of Electronic Equipment Policy is published in its entirety on the CPA's website (www.continuplus.org.uk**).**

Date Policy Created:	**September 2019 (reviewed every year)**
Member of Staff Responsible:	**Sara Devo (Headteacher)**
Review Date:	**September 2022**

Signed: 

(Headteacher)

Signed: 

(Chair of Governors)

Appendix 1

Manager's Guidance Relating to an Investigation

Managers are advised to discuss reporting with Legal and Personnel prior to any investigation taking place.

Producing a report may involve having access to personal information about other workers, particularly when it extends to e-mail. As far as possible such information should be excluded from the report and where this is not possible, the number of people who have access to the information should be kept to a minimum. Legal advice should be obtained to ensure that data protection principles are not breached.

Covert reporting can only be justified if openness would be likely to prejudice the prevention or detection of crime or serious malpractice. The covert watching of another person is not in itself subject to the Data Protection Act; however once it results in a record being kept about the worker, the Act will apply. Under the Regulation of Investigatory Powers Act (2000) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, interception of an unopened e-mail without consent is only permissible under very specific circumstances. Managers must seek legal advice if they plan to intercept e-mail without consent.

The evidence will then be considered and appropriate action taken.

The ContinU Plus Academy

Acceptable Use of Electronic Communications Policy (including ICT Network Use & Data)

From:	
Date:	
I have read and agree to follow the Acceptable Use of Electronic Communications Policy (including ICT Network Use & Data).	
Signed:	