Acceptable Use Policy for C2k Services

The following is the AUP for C2k services which prior to the submission of a new principal form, the principal will be required to accept.

On submission of the request for a new or acting principal, the user will be contacted directly by their local C2k team before being set up in the role as principal.

I, as principal, accept that it is the school's responsibility to adhere to the recommended guidelines below:

General points on use of C2k services

Schools are responsible for having an eSafety policy and an Acceptable Use Policy (AUP) in place, of which all Governors, parents, staff, and students are aware of, as outlined in the Department of Education's eSafety Guidance DENI circular 2013/15:

It is recommended that the policy should state clearly:

- that C2k services are monitored and emphasise the users' responsibilities for the secure use of C2k user names and passwords; for appropriate use of email and the Internet.
- that the school has the right to access user's data and mailboxes. (Requests to c2k to provide access to data will only be actioned if users are aware that this was possible).
- that parents/legal guardians are responsible for their children's out-of-school online use of C2k services.
- that attempts to bypass filtering, or to access inappropriate or illegal material, will be reported to the school authority via C2k.
- the school's BYOD , Social Media & Copyright Policy (DE- Digital Publishing and Software Licensing)
- that email messages are subject to C2k's filtering policy.
- that files stored within the school's network environment on servers, computers and devices will not be regarded as private and that the school reserves the right (*or C2k at school's request*) to monitor, review and examine the internet history, usage,communications and files of all users, and, where it deems it to be necessary,will intercept and delete material on school laptops, servers, network devices and e-mail systems, which it considers inappropriate, and prohibit the use of such material.
- For schools who have opted in to C2k's cloud services: O365 and GAFE - schools must highlight in the AUP the ownership rights of data and the right to access users data if requests to access users data are to be made to C2k.

Note: The C2k's Cloud Service Providers Privacy Policies can be viewed at:

Google Privacy Policy - http://www.google.com/policies/privacy
Office 365 Privacy Policy- www.office365.co.uk/About/Privacy

Sample AUPs are available on the DENI website at: http://www.education-ni.gov.uk/topics/support-and-development and on C2k Exchange

Note: Calls regarding breaches of security, user monitoring or child protection should be logged directly with the Service Desk by telephone: 0870601166.

In order to ensure compliance with Data Protection and/or RIPA (Regulation of Investigatory Powers Act 2000) C2k will require sight of the AUP issued and signed by the relevant individual.

These calls will be marked **Private** and **will not appear in Service Manager**

The school is responsible for ensuring that for :

(a) Info@ mailbox

The school have a policy for the management of info@ emails as the “info@” email address is used by all education authorities to officially communicate with schools. It is recommended that there are 2 info@ recipients to ensure that incoming mail is covered at all time and that schools have an info@ distribution process for forwarding Info@ emails to correct member of staff. For information on info@ management view Quick Check 34

(b) C2k networks

- **Without the specific approval of C2k** :
  - No third party switches are installed in C2k cabinets
  - No third party devices are connected to C2k data points
  - No third party servers or services are installed on the C2k network.
  - No third party user access is provided to C2k Network

  Frequent checks will be carried out to identify any anomalies.

- Any third party software installed on devices on the C2k network should be appropriately licensed. Staff should be made aware of their responsibility to use the software installation facility only for licenced and non-malicious applications, and to ensure that confidential data is not stored on local drives of any computer (desktop or laptop).
- When the school’s C2k Manager, teachers or extended user, install third party local software to individual devices, they adhere to the same standards of security as with every other aspect of the C2k service: desktop software which represents a security threat should not be installed on any device.
- Access to Comms Cabinets should be closely managed by the school to ensure that that C2k’s infrastructure is “not used or altered” by a third party. Any resulting work to address cabinet or C2k network issues by Capita may be chargeable to the school.
- All power and cabling is tested and certified.

(c) C2k usernames

That usernames are available only for current staff and students. *Additional users eg Exam Users, Guest Users and Substitute teachers should be checked on a regular basis by the C2k Manager.*

- Usernames must never be created for fictitious staff or students (this includes the creation of ‘generic’ or group usernames i.e. usernames that could be used by more than one person).
- Leaving dates for students and staff are entered promptly in SIMS.
- Any user under investigation for inappropriate use of the system is disabled promptly.

(d) Nominated Roles (EN047)

- That the users in school nominated roles are correct and kept up-to-date via the appropriate on-line form on C2k Exchange. Roles and nominated users are listed in the Review School Roles
- That The SLT is aware of the role of the C2k Manager (EN072) and which internal roles/ areas of responsibility the C2k Manager can delegate to other staff. (e.g. SMS sender EN017)

(e) Private Folders (EN054)

That Private folders are used for storage of confidential data

- User access to the private folders are managed by C2k on receipt of an on-line form submitted by the principal: “Request for Change for Private Folder Access”

(f) Legacy networks connected to Internet via C2k

All legacy network servers and desktops must have:

- adequate, up-to-date anti-virus protection with automatic updates.
- appropriate, up to date security patches and service packs installed

(f) Insurance and Care of C2k Core Equipment

It is the schools responsibility to take precautions to secure the equipment such as to prevent or at least minimise the possibility of loss of, or damage to the assets. (Refer to EN053 Insurance and Reasonable Care of C2k Equipment)

Please note that C2k core portable devices are only insured by C2k while inside school for thefts or malfunction and not for accidental damage. If the portable device is removed from school, alternative insurance cover must be provided (or replacement liability accepted) both for car and other location. Staff should sign a school’s AUP before taking a portable device outside school. For sample AUP view EN074 AUP for Portable Device.

(g) **Data Protection compliance** - Third Party Data Access and/or Extraction to MIS/SIMS data

Prior to giving data access or extraction permission to a third party, Data Security must be discussed with the school's Data Controller and prior consent given by the school to the supplier when access to or extracting data from MIS/SIMs is required by a third party.

Note: All information is correct at time of issue and EN information sheets accessible while on the C2k school network