Information Sheet EN072

Acceptable Use Policy for C2k Managers

Change requests to add, change or remove a C2k Manager are make by the Principal via an on-line request form. Prior to submitting an on-line form request for a new C2k Manager, the following AUP needs to be read and accepted by the nominated user.

On submission of C2k Manager Change request form, the request is forwarded to Capita to action. On completion of the change request Capita will notify the Principal by email.

I, as C2k Manager, accept that I will adhere to the recommended guidelines below:

The C2k Manager's role involves the management, security and administration of the C2k network services in school on behalf of the school:

The C2k Manager should be aware:

- of the school's Staff and Pupils ICT related AUPs
- respect the privacy and confidentiality of staff and student content and data
- be familiar with the administration structure of the C2k network and have an understanding of how Staff and Student users originate in SIMS

The C2k Manager should make all users aware that:

- C2k services are monitored and should emphasise the users' responsibilities for security of C2k user names and passwords and for appropriate use of email and the Internet.
- attempts to bypass filtering, or to access inappropriate or illegal material will be reported to the school authority.
- that email messages are subject to C2k's filtering policy.

The C2k Manager is responsible for:

- the creation and management of non-SIMS accounts and roving users.
- ensuring that usernames are not 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
- ensuring that enabled usernames are available only for current staff and students
- ensuring that that any user under investigation for inappropriate use of the system is disabled promptly.
- ensuring that, on release of essential updates, the steps provided are followed in order to ensure that the updates install correctly and in a timely manner on all devices.
- managing School and C2k created Groups (egg filtering, BYOD, SMS):
- delegating selected tasks to school nominated staff
- logging calls with the C2k Service Desk
- ensuring that **without the specific approval** of C2k :
  - no third party switches are installed in cabinets
  - no third party devices are connected to C2k live data points
  - no third party servers or services are installed on the C2k network.
  - no third party user access is provided
- ensuring that third party access to the cabinet is closely managed in order to prevent the cabinet and associated cabling being left in a poor state or causing issues which Capita have to address: work required to address such issues may be chargeable

  Frequent checks will be carried out to identify anomalies.

- ensuring that 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

- ensuring that confidential data is not stored on local drives of any computer (desktop or portable devices).

- ensuring that when school staff installs 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.

- ensuring all new power and cabling for C2k network is tested and certified. (EN073)

C2k Managers are by default Service Desk on-line Users (See EN040)

As Service Desk on-line users C2k Manager are able to use the "Service Manager Portal" to:

- log their school's C2k issues on-line
- track progress of their school's tickets on-line
- add updates on-line during the progress of the ticket
- view all on-line tickets logged for their school

C2k Manager/Service Desk Users should not log calls for:

- Breaches of security
- User monitoring reports
- Child Protection issues

Note - Calls regarding breaches of: security, user monitoring or Child Protection should be logged directly with the Service Desk by telephone: 08706011666.

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

For 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.

Training

- Avail of training material in C2k Exchange and Learning Exchange in order to help
  (i) in the day-to-day role in school and
  (ii) to support school users

- avail of training opportunities