System Administrators Charter - Examples

The following examples have been chosen to accompany the System Administrator's Charter [1] to indicate how the charter is intended to work in practical situations.

As I receive enquiries about the charter I will try to update these examples, so if you find an interesting situation which is not covered here, or a case that makes the points better, then please let me know andrew.cormack@jisc.ac.uk [2].

Examples

Modifying or deleting information

Mail loops/quota problems Two common situations cause problems for electronic mail systems: users who forward mail to themselves (thus creating a loop) and users who run out of quota on their inbox. In both cases the mailhub responsible is likely to be affected, potentially degrading the service to other users. This is therefore an operational problem. An authorised administrator is entitled to remove the offending configuration, or move mail out of the full mailbox. A copy of the moved information should be left available to the user, and the user informed as soon as possible.

Deleting messages from mailboxes Administrators are sometimes asked to delete messages from mailboxes belonging to other users. This is almost invariably for policy reasons, and involves the destruction of information held by a third party. Such actions must be authorised individually by the appropriate internal authority, usually the Head of Information Services or equivalent.

Removing published information from a web server Although this is a similar situation to the previous example, there is an additional legal complication. If material that is defamatory, breaches copyright, etc. is published on a web or other server, then the owner of the server may be held liable for the publication. For this reason any organisation with public servers is strongly recommended to have a formal procedure for preventing further distribution of such material if a complaint is received. This is commonly known as a 'notice and take-down procedure'. As there are likely to be legal implications for the organisation, takedown procedures should not be left to system administrators to write. Administrators receiving complaints about defamatory or copyright material on servers should always bring these to the attention of the appropriate internal authorities. File permissions can usually be changed to prevent further publication without destroying the information.

Using logfiles

Investigating service failures The job of a system administrator is to ensure that the system is available for authorised users. Where faults or misuse threaten the availability of the service, for example if there is an unusual load or unexpected failures, then they are expected to investigate this. This is likely to involve examining relevant logfiles or network traffic. As the problems are concerned with the operation of the system, an authorised administrator may investigate without seeking specific permission, however any information discovered that is not relevant to the investigation must be treated as confidential.

Investigating receipt of inappropriate e-mail If a local user complains about a particular e-mail they have received then there should be no problem in requesting their explicit permission for any inspection of their mailbox or files that may be necessary. Checks may also be needed on the logs of mail and other servers through which the message may have passed. If the mail has caused an operational problem then it should be dealt with as described above; if not then it will normally need to be dealt with as a policy matter. Before checking the logs of systems with multiple users, a warning should have been published that the logs may be examined for such purposes. Some e-mails may involve illegal content - these should be reported to the appropriate internal authorities as soon as possible.

Using cache logs to trace fraud A rather common request to operators of web caches and other proxies is to use their logs to trace illegal activity, for example the use of stolen credit card numbers to buy goods. Since such activities are criminal, there should be no difficulty about helping law enforcement officers in their investigations. Note however that data from cache and other logs should only be released through the proper procedure as laid out in section 66 of the Investigatory Powers Act 2016 [3] and our Jisc Guide to disclosing information to law enforcement [4].

Using cache logs to monitor user activity Cache logs can also be a fruitful source of information about user activity but, unless the activity is criminal or has caused an operational problem, such investigations must be treated as a policy matter. Users must therefore be informed in advance that such monitoring may take place. [Note that telling users that cache logs may be monitored may well act as a deterrent to inappropriate activity]. If the administrator is not confident that this has been done they must not obtain or provide access to the information. Logs must only be used as part of specific investigations and not for general "fishing trips".

Monitoring use

E-mail monitoring Some organisations wish to monitor the content of e-mail or other traffic in or out of their networks to check compliance with policies. Users should always be informed of the likelihood of such monitoring as a condition of use of the network. Policy monitoring that results in messages being seen by people other than the sender and recipient is illegal if users have not been informed, and system administrators should not be expected to participate in such monitoring unless they are sure that this has been done.

Screen/keyboard monitoring Systems exist that can remotely monitor the screens and keystrokes of individual workstations. Such systems have the potential to be extremely intrusive and should be implemented, if at all, with extreme caution. One useful application is to allow the user to demonstrate a problem to a remote helpdesk; any such systems should

always be under the user's control and it must be made clear before using them how to start and turn off the remote monitoring. General monitoring of screens and keyboards is currently a legally questionable area: sites wishing to implement it should study the Office of the Information Commissioner's Employment Practice Code [5] (13MB PDF) and in particular Section 3 on Monitoring at Work. Users must be informed of the possibility of such monitoring, and any information obtained must be treated as confidential.

Virus checking Many organisations automatically scan e-mail messages for viruses. If this scanning is done by computers, and provided the process does not reveal the content of messages to administrators or others, then there is no invasion of privacy and no obligation to notify users. However it is good practice to inform users of such systems, if only to forestall complaints when an infected message is detected.

General

Discovering evidence of other breaches It is quite common for authorised administrators to find evidence of problems during normal operations or in the course of other investigations. Where this indicates an operational problem, the administrator may choose to investigate or pass the information to others for investigation. However evidence of policy breaches that do not relate to a current investigation must only be passed to management for them to decide whether an investigation is appropriate. Administrators must not abuse the power and trust given to them by users and management.

Version 1.03

Links
[1] https://community.ja.net/library/janet-services-documentation/suggested-charter-system-administrators
[2] mailto:andrew.cormack@jisc.ac.uk
[3] http://www.opsi.gov.uk/acts/acts2000/20000023.htm
[4] https://www.jisc.ac.uk/guides/networking-computers-and-the-law/disclosure-of-information-to-law-enforcement
[5] https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf