Router configuration

Janet(UK) recommends that you configure your Janet access router to block connections from Janet (and the rest of the Internet) to TCP port 25 (SMTP) of almost all IP addresses in your network. The addresses of a small number of mailers which are carefully managed and are not a relaying risk can then be released from the block; for a small organisation this may be a single IP address.

The commands needed in the router configuration to achieve this blocking vary among manufacturers; the O'Reilly book *Building Internet Firewalls* [1] sets out the techniques in a vendor-independent manner and should enable anyone familiar with your router to implement the filtering you need.

This router blocking gives your organisation some protection against inadvertent relaying when a system is installed or upgraded by non-specialists, possibly in some remote department. It is still wise to disable or correctly configure any mail programs on all systems if you can.

You may also consider preventing outgoing connections to port 25 of addresses outside your own network for all except managed mailers. This will, however, inconvenience your own end users if your security policy otherwise allows them to use their own private Internet accounts from your network and to submit mail to their service provider's mailer. You may prefer to manage the small risk both of relaying by this route and of your users submitting spam by maintaining, publicizing and actively enforcing clear Conditions of Use for your facilities.

Links
[1] http://www.oreilly.com/catalog/fire2/