

# **Westminster Usage and Data Handling Policy**

---

## **Introduction**

Westminster is the Cadet Forces (ACF, SCC, CCF) computer application to administer Adult Volunteers, Cadets and their associated activities. Westminster contains sensitive data, including personal information about adults and children, and access to Westminster is strictly controlled.

This document outlines the security instructions all end users must follow when using Westminster.

An 'end user' is defined as anyone who has been granted a Westminster account.

The amount of data and functionality available to an end user will vary according to the system privileges of the account granted. Only an authorised person may grant or modify a Westminster user account and its privileges.

Please be diligent in this important area.

## **Background**

All end users must observe the Data Protection Act 1998 in relation to the data stored within Westminster. In principle, to meet the requirements of the Act, you must be able to answer 'yes' to the questions below -

- Do I really need this information about an individual? Do I know what I'm going to use it for?
- Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?
- Am I satisfied the information is being held securely, whether it's on paper or on computer?
- Is access to personal information limited to those with a strict need to know?
- Am I sure the personal information is accurate and up to date?
- Do I delete or destroy personal information as soon as I have no more need for it?

Additionally, Westminster is classified as PROTECT – PERSONAL DATA under new Government guidelines. This means that personal data whose release and loss could cause harm or distress to the individuals concerned must be protected.

Personal data includes one or more items from the following list:

- name; address; postcode; email; telephone numbers; driving license number; date of birth; photograph;

Combined with:

- bank or other financial details; National Insurance number; passport number; medical information; place and address of work; conviction; court or similar records; or political affiliations.

OR

- Any of the above collected into a record set of about 1,000 or more records.

All end users must hold a disclosure through the Criminal Records Bureau (CRB) in England and Wales, CRBS in Scotland, and Access NI in Northern Ireland prior to being allowed access to Westminster. An account will not be created unless a disclosure date

has been previously entered into the prospective user's personal details by an end user with necessary authority.

Once an account is set up, an end user will be required to acknowledge that this policy has been read and acknowledged as read before an account can be used for the first time. Users will be prompted by Westminster to re-read and acknowledge this policy every six months or whenever the policy is updated. Access to Westminster is achieved by logging onto the account with a user name and password. Password changes are forced every 6 months.

### **End user security instructions**

- End Users must not disclose their password to others and certainly never display it in a public or obvious place.
- End Users must not use the account of another user.
- Never leave your computer unattended when logged on.
- End Users should only extract personal data from Westminster if there is a legitimate reason (e.g. to manage a training course or send out a mail shot).
- End Users should only extract those personal details required to complete the task at hand and no more.
- End users must delete or destroy all extracted personal data after use. This includes printed paper reports as well as electronically held data. Paper reports must be kept in a locked cabinet until destroyed.
- End users should pass on personal data to other authorised personnel only if it is absolutely necessary and there is a legitimate reason. The recipient should be made aware of the need to protect the data and to destroy it after use.
- End users should not use Westminster in a public place such as an Internet Café, Public Library, or on any other computer of an unknown origin.
- End users must log-out using the Logout menu button after using Westminster even though Westminster will automatically log-out after 30 minutes of inactivity.
- End users must not use the Remember Password feature available in many Internet browsers.

**Extracted data includes all items saved to disk/memory sticks/CDs etc. Sources of extracted data include spreadsheets populated using Export buttons, PDF report files and any other download from Westminster.**

The only browsers that should be used for Westminster are Microsoft Internet Explorer versions 6 or 7. For these browsers, it is your responsibility to set the following options:

1. Open the IE Tools menu, select Internet Options
2. Select the Advanced tab
3. Scroll down to the Security section
4. Select the "Empty Temporary Internet Files folder when browser is closed" checkbox and click OK
5. Select the "Do not save encrypted pages to disk" checkbox and click OK

Paper records containing personal data must be kept in a locked filing cabinet, preferably in a locked room.

### **Security for end user equipment**

Laptops owned by MOD, RFCA and the MSSC which hold or are likely to hold more than 1,000 personal records must be configured with encryption software. The requirement is:

- BeCrypt Disk Protect Baseline V3.1 or higher (software package) or
- BitLocker (software included in Windows Vista) or
- Stonewood Flagstone Baseline. (replacement hard disc) or
- n-Crypt Disk. (replacement hard disc)

Note that the records can be any personal records, including but not limited to Westminster downloads.

It is suggested but not mandated that personally owned computers are also encrypted. Suitable packages are:

- BeCrypt DISK Protect V4.1 or higher
- SafeBoot Device Encryption for PC/Laptop V5.00 or higher
- Commercial versions of Flagstone and n-Crypt

End users on the Army Restricted Network (RLI) should access Westminster using the Internet Gateway Service (IGS) from an MOD approved computer which will be secure and updated regularly. These end users must adhere to current RLI SyOPs and IGS security policies.

All computers accessing Westminster must have anti-virus software installed and regularly updated, and have an active firewall installed and running.

If you use a Wireless Internet connection, it must be encrypted using WPA-PSK or better. See your wireless connection user manual on how to do this.

It is recommended that “password at power-up” feature is set in the computer start up settings. Available on most computers, this usually involves pressing a function key prior to the operating system being loaded and then following the menu prompts. How to do this will vary from manufacturer to manufacturer.

Wherever possible and practical, computers should be shackled to a firm fixing or stanchion using a “Kensington” type security device available from <http://uk.kensington.com>

## Finally

Wherever a security breach is suspected or identified, a Westminster Administrator must be informed at the earliest opportunity with all relevant details of the suspected breach. In all cases, end users must stop using Westminster if something is wrong or suspected to be wrong.

Remember, data security starts with you – it is your responsibility.

Version	Date	Summary of changes	Originator
1.0	15 Feb 08	Initial Release	P Freeman