
## Information Security Document

# Access Control Policy for Volunteers

**Version 9.0**

| Version History | | | |
|---|---|---|---|
| **Version** | **Date** | **Detail** | **Author** |
| 1.0 | May 2013 | Initial Draft for comment in Transformation | Carol Brown |
| 2.0 | Oct 2013 | Incorporating comments | Carol Brown |
| 3.0 | 16/06/2014 | Revised for Information Governance Group | Jo White |
| 4.0 | 14/07/2014 | Approved by Information Governance Group | Jo White |
| 5.0 | 14/09/2015 | Reviewed by Information Governance Group | Jo White |
| 6.0 | 10/10/2016 | Reviewed by Information Governance Group | Jo White |
| 7.0 | 06/11/2017 | Reviewed by Information Governance Groups. No changes. | Jo White |
| 8.0 | 03/12/2018 | Reviewed by Information Governance Group. No changes. | Jo White. |
| 9.0 | 18/12/2019 | Reviewed by Information Governance Group. No changes. | Jo White |
| | | | |

| **This document has been prepared using the following ISO27001:2013 standard controls as reference:** | |
|---|---|
| **ISO Control** | **Description** |
| A.7.1.1 | Screening |
| A.7.2.2 | Information security awareness, education and training. |
| A.9.2.1 > 2 | User registration and de-registration/User access provisioning |
| A.9.2.3 | Management of privileged access rights |
| A.9.2.4 | Management of secret authentication information of users |
| A.9.2.6 | Removal or adjustment of access rights. |
| A.9.4.1 | Information access restriction |
| A.18.2.2 | Compliance with security policies and standards |

## 1 Purpose

Volunteers undertake a variety of roles at the Council and therefore help maintain the level of service provided across Derbyshire. To enable volunteers to perform their role it is essential that they are provided with the appropriate support and training which may in certain circumstances require access to the Council's IT network and systems. This policy details the controls required to be followed for IT network access to be granted in accordance with the Council's Access Control Policy.

## 2 Scope

This policy applies to all managers and staff who have requested or authorised access to the Council's IT network , systems and resources used by volunteers. This policy does not apply to independent or third party volunteer groups who carry out activities in partnership with the Council as these arrangements are subject to separate agreements. This policy must be undertaken in line with all existing Council policies and procedures.

## 3 Policy Statement

Volunteers are not the Council's employees or workers within the meaning of employment legislation and there is no contract of service or contract for services. Volunteers are obliged to comply with the Data Protection Act, Computer Misuse Act and other appropriate legislation during their time with the Council.

Given the status of volunteers, it is essential that all managers give careful consideration to the nature of the IT system(s) to which access is being requested (ie sensitivity of the information within the system) and whether the volunteer's access can be restricted in such a way to ensure that only authorised activities can be performed under the assigned volunteer's user account. This could be facilitated by providing the minimum system requirements for the task(s) to be undertaken at the point that the request is made. It is not acceptable for volunteers to be provided with access to any of the Council's IT systems that are deemed to contain sensitive or personal information or be provided with transactional permissions for any finance system. It is also essential that prior to the volunteer accessing the Council's IT network they are made fully aware of their obligations under the Data Protection and Computer Misuse Acts. Where appropriate a non-disclosure agreement should be completed.

Managers requesting volunteer access to the Council's IT network and systems must ensure that they have taken all reasonable steps, ie induction and training, to ensure that the volunteer is fully aware of their individual responsibilities when accessing the Council's IT network. In the event that a volunteer accidentally or intentionally discloses their user account credentials or other information obtained as a result of their access to the Council's IT network then access to the Council's IT network and systems may be withdrawn.

Managers must ensure that they are fully aware of the Council's information security policies and procedures and conduct appropriate induction and regular training for all their staff including volunteers. Volunteers should not be assigned responsibility for Council IT equipment including PCs or laptops.

All volunteers will be required to agree the following policies when first accessing the Council's IT network as part of their 'Volunteer's Agreement' with the Council.

- Safe Haven Guidance
- ICT Acceptable Use Policy
- Internet and e-mail Acceptable Use
- Password policy

The authorising manager is responsible for determining the level of access to systems and data required in order for the volunteer to undertake the tasks required. The accounts will **not** be created by cloning an existing account but must be detailed individually.

To provide a clear audit trail of volunteer activities on the Council's IT network and maintain the integrity of such systems. Managers must request and allocate a volunteer account to each individual and not allow the sharing of user accounts. The request should be made using the template available on Dnet or Service Desk on line.

The request will be shared with the appropriate Departmental Service Relationship Manager who will need to acknowledge the request. This is an important control in the process and should be used as an opportunity to independently assess the request and challenge the requirement if appropriate.

All such accounts will be set up to expire within 3 months of creation, unless the volunteer access requirement is for a specified time period of less than 3 months. In the event that the volunteer's access is required beyond the initial 3 month period, this will need to be authorised by the requesting manager in blocks of 3 months.

In the event that the volunteer's user account requires a password reset either during the initial distribution of the password or at a later stage the authorising manager will need to contact the Service Desk. To validate the request, the authorising manager will need to complete the security check process before handing the phone to the volunteer so that the Service Desk can pass on the new password details. The password will be set so that it requires changing after first logon.

The account will be set up as 'Volxxxx' with xxxx being a number which is incremented by one for subsequent accounts. The volunteer's name will be recorded in the related surname and first name fields.

The volunteer accounts will be held in the external domain and must be deactivated and removed when no longer required.

## 4 Breaches Of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.

All Council employees, elected members, partner agencies, contractors, vendors and volunteers have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of a member of staff the matter may be dealt with under the disciplinary process. In the event that the issue relates to the actions of the volunteer, this may be dealt with by withdrawing the volunteer's access to systems or by asking the volunteer to stop providing the activity.

As volunteers are not employees of the Council, the Council's disciplinary and grievance procedures are not available for the volunteer. However, if the Manager has failed to properly induct or train the volunteer, this may constitute a disciplinary matter.

***This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.***