ICT Policy

Policy Statement

This policy sets out Refugees Welcome's policy in relation to the use of ICT and the maintenance of secure systems to provide for appropriate confidentiality and data sharing.

All Trustees, Contractors, Advisors and Volunteers are required to abide by this policy.

The policy applies to all use of technology by Trustees, Contractors, Advisors and Volunteers, and if appropriate to users of the service.

[Volunteers to be referred to the GDPR Policy, Confidentiality & Information Sharing Policy, Social Media Policy, Volunteer Guidelines and Volunteer Confidentiality Agreement)]

Policy date: May 2020
By: Anne Towers – Trustee/ Alex Major CVSCE
Status: Final

Policy

Refugees Welcome recognises the importance that all of its systems are protected to an adequate level from vulnerabilities.

Such risks include accidental data change or release, malicious damage (internal or external), fraud, theft, failure and natural disaster.

It is important that a consistent approach is adopted to safeguard Refugees Welcome's information in the same way that other more tangible assets are secured, with due regard to the highly sensitive nature of some information held on both electronic and manual systems.

As well as a common law duty of care, Refugees Welcome has a legal obligation to maintain security and confidentiality for the data it holds, this is included in our GDPR policy.

It is the duty of Refugees Welcome and its Trustees, Contractors, Advisors and Volunteers to meet these legislative and regulatory requirements in relation to Information and Communication Technology (ICT) Security.

This policy sets out the procedures to be followed by all Trustees, Contractors, Advisors and Volunteers to ensure that Refugees Welcome's ICT assets — hardware, software and data — are protected.

It is aimed at ensuring:

- Confidentiality: data access is confined to those with specified authority to view the data
- Integrity: all systems are working as they were intended to work and all data protected from unauthorised change
- Availability: data is available to the right person, when needed

The need for a Security Policy

Data stored in information systems represent an extremely valuable asset. The increasing reliance of Refugees Welcome on ICT for the delivery of its services makes it necessary to ensure these systems are developed, operated, used and maintained in a safe and secure fashion.

The increasing need to hold personal data for contracting and service delivery and transmit this information across ICT systems by Refugees Welcome renders data more vulnerable to accident or deliberate unauthorised modification or disclosure. The use of computers to exchange data electronically offers advantages to Refugees Welcome if handled securely, but could present serious hazards if security is inadequate.

This policy applies to all Refugees Welcome Trustees and Volunteers, also Contractors or Advisors but working on behalf of the organisation. It also applies to all areas of Refugees Welcome's activities so covers all Information Assets, be they Volunteer or Service user related, or not.

Refugees Welcome has made a firm commitment to monitor and protect its confidential information. This may be person identifiable information relating to volunteers and users of the service or it may be documents of a commercially confidential or sensitive nature.

It has, therefore, become a fundamental principle of Refugees Welcome to have an effective and consistent ICT Security Procedure in place.

Duties and responsibilities

The Trustee Board of Refugees Welcome has responsibility for all elements of data protection and security of information. Matters of exception are reported to the Board of Trustees who have oversight for this.

Their duties in relation to ICT Security include:

- Contract with CVS Cheshire East for the use of their secure 'Teams' system
- Periodically report to the Board of Trustees the state of ICT security
- To keep up to date with new developments and requirements to ensure the ICT security policy remains current
- Ensure that ICT security policy is implemented
- Ensure compliance with relevant legislation including GDPR as set out with Refugees Welcome GDPR policy
- Help ensure that all Trustees and volunteers are aware of their security responsibilities and providing support and guidance for all users including periodic access to online safety training.
- Assist with Internal Audit plans to review Refugees Welcome's compliance with any external contractual security policies (e.g. CEC and CVSCE security policies)
- Recommend software / hardware purchases in the organisation as needed.
- Comply with ICO registration

All Trustees and volunteers are responsible for ensuring that they comply with Refugee Welcome's information security requirements, including ensuring they apply the standards set within the ICT Security policy and procedures.

Procedures

Refugees Welcome physical and data assets associated with its information systems:

Physical Assets

- Currently Refugees Welcome does not own any physical IT assets. However, should we have equipment to loan out, each physical asset would be assigned an "owner". The owner of all physical assets (computer hardware and associated peripheral equipment) would be Refugees Welcome but for practical purposes (security marking, inventory, maintenance etc.) would be delegated to the 'owner'.

Software Application Assets

- Refugees Welcome would hold copies (or evidence) of relevant licences and guarantees.

Access Control for Data Systems

- A key element of ICT Security is ensuring suitable controls are in place to restrict access to those who need it. Also, it is important to ensure that measures are in place to prevent misuse or theft of the relevant assets.

Refugees Welcome's Systems

- Refugees Welcome via CVS Cheshire East is responsible for leading on security for all the Refugee Welcome-wide electronic systems, including the maintenance and developments of related procedures and policies. Special attention will be given to the allocation of "privileged" or "supervisor" rights, which will normally be available only to certain members of the Trustee management team on a 'need to know' basis.
- To access any 'Information Asset' the user must first have an authorised and active CVSCE/Refugees Welcome 'Teams' user account, which will be approved by the Volunteer Programme Manager. Access to the Database will be actioned by the CVSCE Volunteer Co-ordinator and or the Volunteer Programme Manager.
- Only key volunteers and named Trustees have access to Refugees Welcome 'Teams' site managed by the CVS Cheshire East.
- Levels of access will be set by Refugees Welcome and will be maintained by Refugees Welcome in partnership with the CVS Cheshire East. They will be responsible for:
    - keeping a record of all users for each system
    - removing the access rights of any Trustee / volunteers who have changed role or left the organisation
    - periodically checking for and removing redundant accounts that are no longer required
    - ensuring all users' access rights will be reviewed periodically to ensure that access levels remain consistent with their duties.

- In gaining access for users the Volunteer Programme Manager or Volunteer Co-ordinator will check that the level of access requested is consistent with organisational security policies (See Appendix 1)

Password management

All ICT systems will have a password function and no lists of passwords for Trustees or volunteers will be stored on the system.

In setting passwords and communicating these to new Trustees and volunteers or sending reminders, no single email will contain both the username and password.

All systems used by Refugees Welcome which hold personal data will have an individual username and password to access the system. There will be no group accounts. This is to ensure that there is accountability and transparency in the use of the system and limit the potential for accidental disclosure of passwords.
Passwords will:

- Be complex and contain at least 7 characters with, at least one upper case letter, one number and one symbol.
- Allow users to select and change their own password and include a confirmation process to check for spelling errors
- Not display password on the screen while typing
- Limit the number of incorrect logins to 3 with the account being locked out and administrator being contacted
- 'Timeout' to log users out when not at their computer

All new Trustees and volunteers should be briefed on the importance of passwords and instructed in the manner in which they are to be used and protected as part of the Trustees and Volunteers induction process where appropriate and necessary.

Equipment Security

Refugees Welcome (via CVS Cheshire East) is a cloud based organisation and so does not manage or maintain any servers or business critical equipment on its sites. Trustees and volunteers are required to use a laptop/computer in fulfilling their role which is provided by themselves.

Refugees Welcome will ensure that:

- If laptops are provided they will be all installed with virus protection software
- Refugees Welcome does not allow the use of USB or data transportation of sensitive data.
- Via the CVS Cheshire East any maintenance arrangements that are the subject of contractual agreement have only approved system engineers accessing
- Each individual laptop would have an individual secure login with a password to access the PC.

Refugees Welcome (via CVS Cheshire East) contracts with a third party IT provider to support with the security of the ICT systems.

It is the policy of Refugees Welcome that Trustees and volunteers are not authorised to store any personal client data on the hard drives of their computers. All data is stored on the 'Teams' system which is secured with a 30 day back up.

Disposal of ICT equipment
When a laptop/desktop computer becomes obsolete or is broken beyond repair then all data is removed from the hard drive including the operating system. The hardware will then be disposed of through appropriate methods.

Procurement of Physical Assets
All security requirements should be identified at the requirements phase of a project and justified as part of the procurement process.

- All procurements will be considered and approved by the Refugees Welcome Trustee Board.

In the acquisition of new hardware or systems the Trustee management team would consider:

- any new ICT facilities provide an adequate level of security
- as defined above, and desirable security requirements are included in procurement specifications
- Suitable back-up and disaster recovery procedures will be in place as supplied by CVS Cheshire East for Data systems

Training Requirements

All Trustees Contractors Advisors, and Volunteers will made aware of this policy and related ICT security polices listed (GDPR, Confidentiality and Information Sharing and Social Media policies). Trustees and volunteers will also receive training in any specific systems they will use as part of their role which will reinforce any security requirements.

POLICY DATED: May 2020

ADOPTED ON: 10.6.2020

REVIWED: May 23

SIGNED BY: N.A. Campbell CHAIR of TRUSTEES DATE: 20.4.23

NEXT REVIEW DATE: May 2024

Appendix A – Access levels in Systems

Name of System	Level of access	Typical role with level of access
Refugees Welcome (visa CVS Cheshire East 'Teams' secure system)	Access to Refugees Welcome- Casework, Resources and Volunteers Information	Volunteer Supervisor Volunteer Programme Manager Trustee