Herts &
Middlesex
Wildlife Trust

IT Acceptable Use Policy (ITDP_P4)

Document version:	V3
Policy owner:	Head of Business Support
Next policy review date:	September 2025
Approved by HMWT Council on:	9 December 2011 (meeting C/234)
Signed:	
Print name:	Mike Master
Position:	Chairman
Reviewed:	June 2021 (C/274) September 2022 (C/279)
Amendments:	Update to whole policy following IT infrastructure upgrade and changes to Data Protection Policy. Details taken out and merged into Data Protection and Use of IT Guidance document. Adapted to new policy template. General review and update.

Introduction

Information technology (IT) is vital to the efficient performance of Herts & Middlesex Wildlife Trust and this policy applies to everyone who has access to and uses any of the IT systems provided by the Trust.

Staff, volunteers and other users must recognise acceptable practice in all aspects of IT and use the systems in a professional, effective way both for the safety of the user and organisational security.

The Trust is a ‘Data Controller’ for the purposes of the Data Protection Act 2018 which is the UK’s implementation of the General Data Protection Regulations (GDPR). The Data Protection Act 2018 covers the use of all information about identifiable living individuals (‘personal data’) which is stored/processed by computer or a structured manual filing system, and is covered by the Trust’s **Data Protection Policy (DP_P1)** and **Privacy Policy (DP_P2)**.

Where there is irresponsible or illegal use of, or failure to take reasonable care of, the Trust’s IT systems, or misuse of IT in a manner that could bring the Trust into disrepute, subject the Trust to a fine from the Information Commissioner’s Office (ICO) or put the organisation at technical or commercial risk, disciplinary action may be taken against staff or volunteers may be asked to step down from their role.

All individuals are responsible for adhering to this policy. Staff and volunteers must ensure that those individuals who do not have access to the **IT Acceptable Use Policy (ITDP_P4)** and supporting document – **Data Protection and Use of IT Guidance** (i.e. guests, non-office volunteers) are instructed on how to access the Trust's IT systems in line with the policy and guidance.

1. Access to the Network and Internet Security

Network access is heavily restricted to only those individuals who require access in order to carry out their work. Remote connection to the Trust's network is only available to authorised users. The Head of Business Support, in conjunction with the Senior Management Team, authorises which users should be granted network access.

The Trust strives to keep its computers and network free of viruses and other malware. Virus protection is employed on the Trust's IT resources at all times and updated as defined by the IT support company.

To ensure that the Trust network remains virus-free, procedures specified in the **Data Protection and Use of IT Guidance** must be followed at all times. Staff and volunteers must be vigilant at all times in order to protect the Trust's IT resources.

Any doubt about the validity of a file or other media must be checked with the Head of Business Support or the IT support company immediately.

The IT support company is responsible for ensuring a complete and accurate patch management process is carried out on the network and with all associated software programs.

Mobile devices such as USB drives, CDs, DVDs and removable hard drives must only be used in situations where network connectivity is unavailable or there is no other secure method of transferring data, and in this case only Trust authorised mobile storage devices with encryption enabled must be used.

User passwords must not be disclosed to anyone. Passwords are changed periodically as per the password protocol outlined in the **Data Protection and Use of IT Guidance**.

2. Use of Email, social media and the Internet

All staff and volunteers must follow Trust guidance on the appropriate use of email and social media to communicate and deliver their activities.

Use of the Internet by Trust staff and volunteers is permitted and encouraged where such use is suitable for business purposes and supports the aims and objectives of the Trust.

All staff and volunteers must follow Trust guidance which outlines restrictions for internet use either on Trust property or whilst carrying out activities for the Trust.

3. IT Hardware

The Trust provides IT equipment and training for users, as required. Equipment is provided for business use and must be treated with care and maintained in accordance with manufacturer's instructions and Health & Safety guidance.

Mobile devices used for banking and payments (i.e. banking card reader, iZettle terminal) must only be used by authorised individuals.

DSE (Display Screen Equipment) assessments must be completed for workstations in the office and at home for DSE users as set out in the Trust's DSE Policy.

Personal devices (i.e. personal laptops) can be used but must have up-to-date anti-virus and be running a current and supported version of a Windows Operating System. The Trust is not responsible for non-Trust equipment or its damage when attached to any piece of the Trust's IT infrastructure. Repair and maintenance of non-trust IT equipment is not covered under the Trust's IT support contract.

All IT equipment must be kept secure at all times, at Trust property, whilst being transported, or used elsewhere. Access to equipment will be restricted and monitored accordingly.

When taking a device or storage media off-site, individuals must continue to abide by Trust policies and guidance.

Redundant IT equipment will be disposed of in accordance with the WEEE directive and a certificate of destruction is issued. Equipment owned by the Trust must be returned to the Business Support Team who will organise disposal.

4. IT Software

Only software programs bought by, developed for, or legitimately acquired by the Trust may be run on Trust hardware. Only the Trust's IT support company are authorised to install and deploy software and approval is required from the Head of Business Support ahead of any software installation

Deliberate unauthorised access to, copying of, alteration to, or interference with software programs or data is not allowed, and can constitute an offence under Copyright and Computer Misuse legislation.

5. Data Back-Up and Disaster Recovery

The Trust has a robust Disaster Recovery procedure which is managed by the IT support company. This is supported by data backups.

6. Resources

For further guidance for staff and volunteers, please refer to the **Data Protection and Use of IT Guidance** document.