IT Acceptable Use Policy

Revision V4.0

Last revised: November 2024

This policy should be read in conjunction with other relevant policies, procedures and Codes of Conduct including:

- Online Safety and Social Media Policy
- Disciplinary and Grievance Policy.

Volunteers and employees should be given sufficient training and knowledge to be able to recognise and report potential misuse and to enable them to use software and systems as relevant to their role.

This policy applies to all users whether employed by Manvers Waterfront Boat Club (MWBC), external contractors providing services on behalf of MWBC, volunteers and other individuals who work for or provide services on behalf of the MWBC. These individuals are collectively referred to in this policy as users.

The policy applies in respect of all ICT resources and equipment that have been made available to users for working at home. ICT resources and equipment includes computer resources, use of MWBC internet access and email systems, software (including use of software such as Webcollect), cameras and recording equipment and any other electronic or communication equipment used in the course of the user's work. This policy also provides advice to users in respect of the potential risks and consequences in relation to inappropriate use of their own personal ICT facilities, where this use is inconsistent with the expectations of users working with children and young people.

Access
Users will be provided with a login where they are entitled to use MWBC ICT facilities and advised what hardware and software they are permitted to access, including access to the internet and email. Unless indicated, users can use any facilities available subject to the facilities not being in use by other colleagues. Access is provided to enable users to both perform their role and to enable the wider club membership to benefit from such facilities.

Where users have been provided with a MWBC email address to enable them to perform their role effectively, it should normally be used to communicate to members.

Some users may be provided with laptops and other equipment for the performance of their role. Where provided, users must ensure that their laptop/other equipment is password protected and not accessible by others when in use at home and that it is not used inappropriately by themselves or others. Users must also ensure that they bring their laptop/equipment in as required for updating of software, licences and virus protection.

Users who have access to members personal contact details must ensure that they are kept confidential.

Users are advised that inappropriate communications that come to the attention of MWBC can lead to disciplinary action.

Users should refer to the Online Safety & Social Media Policy which contains detailed advice on the expectations of volunteers and members when using social media.

Unacceptable Use
MWBC systems and resources must not be used under any circumstances for the following purposes:

- to communicate any information that is confidential to MWBC or to communicate/share confidential information which the user does not have authority to share.
- to present any personal views and opinions as the views of MWBC to make any comments that are libellous, slanderous, false or misrepresent others.

- access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material.
- communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally.
- to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
- collect or store personal information about others without direct reference to the Data Protection Act.
- To use MWBC's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised project.
- To use MWBC's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by MWBC.
- to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.
- Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal.
- If users are unsure about the use of ICT resources including email, advice should be sought from the IT Officer.
- Where an individual accidently accesses a website or material that they consider to be pornographic or offensive, this should be reported immediately to the IT Officer, Club Secretary or other member of the committee.

Personal and private use

All users with access to computer equipment, including email and internet, are permitted to use them for occasional personal use provided that this is access is not:

- involving the use of news groups, chat lines or similar social networking services.
- at a cost to MWBC.

Security and confidentiality

- Any concerns about the security of the ICT system should be raised with a member of the committee.
- Users are required to ensure that they keep any passwords confidential, do not select a password that is easily guessed and regularly change such passwords.
- Users must take account of any advice issued regarding what is permitted in terms of downloading material to MWBC's server.
- Users must ensure that their use of MWBC's ICT facilities does not compromise rights of any individuals under the Data Protection Act. This is particularly important when using data off site and electronic data must only be taken off site in a secure manner, either through password protection on memory pens or through encrypted memory pens. This is also particularly important when communicating personal data via email rather than through secure systems. In these circumstances, users must ensure that they have the correct email address and have verified the identity of the person that they are communicating the data with.
- Users must also ensure that they do not compromise any rights of individuals and companies under the laws of Copyright through their use of ICT facilities.

Monitoring

MWBC reserves the right to monitor the use of email, internet and intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- to ensure that the security of MWBC's hardware, software, networks and systems are not compromised.
- to prevent or detect crime or unauthorised use of MWBC's hardware, software, networks or systems
- to gain access to communications where necessary where a user is absent for a period of time.
- To protect the right to privacy, any interception of personal and private communications will not take place unless grounds exist to show evidence of crime, or other unlawful or unauthorised use. Such interception and access will only take place following approval by the committee.

Whistleblowing and cyberbullying
Users who have concerns about any abuse or inappropriate use of ICT resources, social networking sites, email or internet facilities or inappropriate communications, should alert the committee to such abuse.

Data security
To avoid a risk of confidential information being disclosed to unauthorised third parties:

- Logout of remote access before leaving the computer.
- Use a password protected screensaver to prevent anyone gaining access to the computer.
- Do not reveal passwords.

Users must comply with the terms of this policy. Any breach will be considered to be a breach of disciplinary rules, which may lead to withdrawal of access to ICT facilities. Users should be aware, that in certain instances, inappropriate use of ICT may become a matter for police investigations.