


Integrated Management System	C10	
Acceptable Use Policy for WRAP IT Systems		
Version: 4	Date: November 2021	Page 1 of 10

1 Introduction

1.1 Scope

This Acceptable Use Policy for IT Systems sets out the ways in which technology may be used within WRAP, applies to all users and is designed to protect WRAP, our employees, funders and other partners from harm caused by the misuse of our IT systems and our data.

1.2 Purpose

To ensure that all staff understand what is acceptable and unacceptable use of IT systems.

1.3 Contents

Contents

1 Introduction	1
1.1 Scope.....	1
1.2 Purpose	1
1.3 Contents.....	1
1.4 Definitions.....	2
2 General	2
2.1 Individual's Responsibility	3
2.2 Use of IT Systems.....	3
2.2 Use of Personal Devices	5
2.3 Remote Working.....	5
2.4 Use of Data Storage Devices	6
2.5 Data Security.....	6
2.3 Use of Internet.....	7
2.4 Installation of Software.....	8
2.5 Configuration Changes	8
2.6 E-Mail Security	8
2.7 Telephones.....	8

2.8	Personal Data	9
2.9	Environmental Considerations	9
3	Enforcement	9
4	Access by Administrators	9

1.4 Definitions

“Users” are everyone who has access to any of WRAP’s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, funders, customers and business partners.

“Systems” means all IT equipment, software, Internet technology, video or voice equipment that connects to the corporate network, has access corporate applications or has been supplied or installed by WRAP.

This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, personal devices, home computers and all other similar items commonly understood to be covered by this term.

“Data” means any electronic information of any kind.

“Data store” means any device, network drive or cloud-based area for the purpose of storing data.

“Password” means any sequence of characters or PIN number used for the purpose of verification

2 General

This is a universal policy that applies to all Users and all Systems.

This policy covers only internal use of WRAP’s systems, and does not cover use of our products or services by customers or other third parties. The policy is used in conjunction with the Computer Misuse Act 1990 and the Data Protection Act 1998.

Where aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Where there are additional policies that overlap with this policy (e.g. data handling) then the additional policy has precedence but both policies will apply in all cases.

2.1 Individual's Responsibility

User Accounts

All staff members at WRAP are responsible for monitoring and enforcing compliance with this policy and all staff are responsible for ensuring that they remain compliant with relevant local and national legislation at all times.

All users are issued with uniquely assigned ID's which are used to control access to WRAP's IT systems. A user must never allow another person to use any of their ID's and all users remain accountable for any activities undertaken within the auspices of their assigned ID's.

All user ID's are password controlled and users must set their own passwords, which must not be simple passwords¹, and never reveal their passwords to anyone else, other than in the circumstance of IT support by WRAP staff whereupon the password must be changed immediately afterwards.

Access

Users must take all necessary precautions to protect access to systems and should never leave systems logged in when not required.

Screen locks must be applied when a system is left unattended.

Laptops and mobile devices must never be left unattended in public and if left in vehicles must be obscured from view. Bags that are easily identifiable as laptop bags must never be left on view in unattended vehicles.

Breaches

Where a user believes or notices the existence of any security breach the WRAP IT department must be notified immediately.

2.2 Use of IT Systems

By logging in or connecting to a WRAP system users are inherently agreeing to the following:

By clicking on the OK button below and logging into this machine, you agree to abide by the terms of the WRAP acceptable use policy. A copy of this policy can be viewed on the intranet or by raising a service request. The Information Systems department reserves the right to monitor and audit your activity on this machine. Users are responsible for ensuring they act in accordance with the acceptable use policy, and those laws and legislation applicable to the WRAP network and in local jurisdictions. Unauthorised access to this system is strictly forbidden.

¹ A simple password is any that does not have at least: i) 8 characters, ii) one lower case and one upper case character, iii) a numeral OR a punctuation character

All data stored on WRAP's systems is the property of WRAP. Users should be aware that the company cannot guarantee the confidentiality of information stored on any WRAP system except where required to do so by local laws.

WRAP's systems exist to support and enable the business and must not be used for personal activities or in support of another business, company or organisation.

No data should be removed from any WRAP system unless there is a reasonable business imperative to do so.

WRAP can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

WRAP reserves the right to regularly audit networks, devices and systems to ensure compliance with this policy.

Code of Conduct

Users of WRAP systems are expected to access, download or process material directly related to their work only. It is not acceptable to access, download, create, edit or process any offensive material that includes, but is not limited to:

- any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others;
- unsolicited "nuisance" emails;
- material which is subsequently used to facilitate harassment, bullying and/or victimisation of a member of staff or a third party;
- material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;
- material with the intent to defraud or which is likely to deceive a third party;
- material which advocates or promotes any unlawful act;
- material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or
- material that brings, or may bring, WRAP into disrepute.

The WRAP network must not be deliberately used by a member of staff for activities having, or likely to have, any of the following characteristics:

- the intentional waste of staff effort or other WRAP resource;
- the corruption, alteration or destruction of WRAP data without due authority;

This document is uncontrolled if printed

- the disruption of other staff members or the correct functioning of the WRAP Network;
- the denial of access to the WRAP network and its services to other users or parties;
- pursuance of commercial activities not authorized by WRAP;
- the avoidance or abuse of copyright or the use of commercial services without adequate payment;
- torrent or other streaming;
- the broadcast of radio signals or other interruptive services;
- access or attempt to access data, systems or other resources to which permission has not been formally granted;
- any activity that weakens, or may weaken, WRAP's data, network or system security
- personal activities or the use of social media beyond infrequent and brief activity;
- the subversion, hacking or illegal access to any network or resource on the Internet

Accidental Access

Where material which contravenes the Code of Conduct and is inadvertently accessed the Head of Information Systems should be notified immediately with a URL, date and time. Failure to do so will deem such access as intentional.

2.2 Use of Personal Devices

Personal devices (e.g. mobile phones, tablets, home PCs) may be used to access the WRAP e-mail system but may not access any other WRAP IT systems or data other than those made available through a mobile client application, such as SoonR.

WRAP data, other than e-mail or that made available through a mobile client application, must not be stored on or downloaded onto personal devices. This includes home computers, portable storage devices and memory sticks.

WRAP provides the BYOD Wi-Fi network in offices and users may connect their personal devices to this network using their WRAP credentials. Personal devices must not be connected to the WRAP wired or other WRAP Wi-Fi networks.

2.3 Remote Working

Accessing WRAP systems remotely across the Internet using the WRAP Virtual Private Network (VPN) client is permissible for all staff who have been authorized to do so. Authorised staff are those that have an account that allows such access.

Use of the VPN is only allowed on a WRAP owned device. The VPN may not be used on any personal or home devices.

When travelling all WRAP devices must be taken as hand luggage. When accessing data in a public place care must be taken so that strangers cannot read screens or printed materials.

2.4 Use of Data Storage Devices

WRAP provides all users with high quality networked storage systems (e.g. W: drive, SoonR) and data should be stored in these since they are robust, backed up and secure. Data should not be removed from WRAP servers unless there is business imperative which justifies such removal – for instance, the presentation of PowerPoint on a different computer.

In general, the use of memory sticks should be avoided for anything other than the temporary transfer of data that has no sensitivity to WRAP and is of no importance if lost.

2.5 Data Security

WRAP takes the security of its data very seriously and maintains a number of data handling policies.

Sensitive Data

Sensitive data is registered in the WRAP Data Register and must be only stored on the S: drive.

Data classified as sensitive is subject to one or more of: i) legislation such as the Data Protection Act, ii) contractual obligation such as data given to WRAP by partners, iii) competitive advantage such as future company strategies, iv) company reputation and iv) personal information such as bank account or contact details.

Whilst the Data Protection Act does not apply to corporate data WRAP has decided to apply its principles to all data. Staff cannot therefore share any sensitive data without the express written agreement of the registered data controller and any such agreement must be recorded in the data log.

No data that has any characteristics of sensitive data can be removed or copied from the S: drive, printed or referenced unless particular dispensation has been given by the data controller. Where additional data encryption is required WRAP provides the Sophos encrypt utility for staff to use.

Data Privacy

Staff will, in general, keep WRAP data private unless there is an acknowledged agreement to share data. If there is doubt then the Data Protection Officer should be consulted.

Once data is shared WRAP loses control of that data and its privacy can no longer be guaranteed.

Personal versus Corporate

Personal data storage utilities, websites, hardware, systems and devices must not be used to store WRAP data. It is important that staff clearly distinguish between personal systems and WRAP systems.

Data Sharing Utilities

WRAP provides the SoonR system to enable data sharing with external parties. This utility allows the tracking and control of data sharing and can be used to provide or receive data to/from external parties. Care should be exercised when using the 'anonymous' data sharing facility and any data shared anonymously must have an automatic termination date.

It is not permissible to use Dropbox, Box, OneDrive, iCloud, GoogleDrive or any other online or cloud data storage utility to store WRAP data.

Sharing Data with External Parties

Where data is shared with external parties it must be fully auditable such that it is clear what was shared with whom and at what dates and times.

Social Media Data

The use of social media data is covered by the WRAP Social Media Policy.

Anti-Virus

Where WRAP has installed anti-virus or other protective software this must be left to work undisturbed and may not be uninstalled. If a virus file is detected users must not remove them themselves but alert the IT Department.

2.3 Use of Internet

WRAP provides Internet access to all staff for the benefit of the business and it may not be used in any other capacity. Occasional private use is tolerated but such use must not distract from the delivery of WRAP business nor deteriorate network or bandwidth capacity.

Internet Content

The access of Internet content is monitored and filtered such that any illegal, pornographic, immoral, copyright infringed or offensive content is blocked. However, it is impossible to block content of this nature comprehensively and staff must not attempt to access, print, download or view any content of this nature. It is possible to accidentally access such content and in this event the IT department should be notified immediately.

Where users are proven to be the cause of any copyright cease and desist orders then WRAP reserves the right to pass any costs across to that user.

2.4 Installation of Software

WRAP's laptops and servers have been built and configured to uniform standards. WRAP staff are given privileged access to their own laptops so that they are empowered to make urgent changes whilst away from the office. However, users must not install or attempt to install applications without first discussing the installation with the IT department. All licensed programs are managed by the IT department and only the IT team are permitted to apply a WRAP purchased licences.

The installation of apps on WRAP smartphones is an exception and users may, using their own judgment, install such apps that they need in order to conduct WRAP business.

2.5 Configuration Changes

Users must not change or attempt to change the configuration of laptops, servers, telephones, TVs, Video Conference units or other device. Users may change the configuration of WRAP smartphones that have been issued to them such that it enhances their efficiency.

All WRAP laptops have encrypted drives which must never be unencrypted.

2.6 E-Mail Security

E-mail attachments present the single greatest current threat to the security of WRAP's infrastructure and electronic investment. Users must take great care when opening attachments in e-mail.

2.7 Telephones

WRAP provides users with fixed landline and mobile telephones in order for them to deliver company business. All phones are able to make international and premium rate phone calls and all WRAP phones have fully logged calls.

Users are trusted to make such telephone calls that are requisite to their deliver of business and are expected to exercise reasonable judgment on the value of a call

against cost. For clarity, calls to UK landlines and UK mobiles are free from WRAP landlines. Calls to UK landlines and UK mobiles are free (within a 4 hour total monthly limit) from WRAP mobiles whilst connected to UK networks.

It is anticipated that users will make a small number of personal calls using landline and mobile phones and this is perfectly acceptable for all free calls. It is also anticipated that users may need to make a personal call that isn't free, particularly when travelling abroad on behalf of WRAP, and users are expected to draw attention to this and reimburse the company for the costs of those calls.

2.8 Personal Data

Users may not store personal data, music, photographs or other items on WRAP equipment or data stores. Whilst WRAP provides each member of staff with a personal drive this area is not to be used for the storage of personal data but the management of WRAP data that is not ready for or shouldn't be released to colleagues.

2.9 Environmental Considerations

Users are encouraged to reduce the power consumption of all devices by turning them off when not in use. Monitors on desks should be turned off when not in use.

3 Enforcement

WRAP retains the right to examine any systems, data or devices that it owns or is under its administration or supervision.

Where use of WRAP systems has been formally deemed unacceptable WRAP will take appropriate disciplinary action.

WRAP retains the right to monitor all electronic activity and transactions within its network and systems.

4 Access by Administrators

Where staff have administrative access to a system or device any such access must be used judiciously. Administrators are not permitted to examine, view, copy or edit data that they have no rights over or data that is in any way sensitive or secure. Staff must not abuse administrative rights and must not attempt to change permissions or access in order to circumvent such permissions.

In general administrators will be given a standard user account and an administrative account and all administrative activities must be conducted using the administrator account.

It is not permitted to generate generic accounts with administrative enablement.

Where such business priorities require an administrator to access a user's e-mail or personal data the administrator must ensure that authorization has been sought from the user's line manager and that the user is informed of the incursion.