Lee Valley Regional Park Authority	Agenda Item No:
LEE VALLEY REGIONAL PARK AUTHORITY	7
AUTHORITY MEETING	Report No:
28 APRIL 2016 AT 14:00	A/4225/16

I.T USAGE POLICY REVIEW

Presented by the Director of Finance & Resources

SUMMARY

This report sets out proposed changes to the Authority's I.T Usage Policy.

Members of the Executive Committee considered the proposed changes and additions to the I.T usage Policy at their meeting earlier today (Paper E/445/16). An oral update of their recommendations will be given at the Authority meeting.

RECOMMENDATIONS

Members Approve:

(1) the changes and additions to the I.T Usage Policy as set out at Appendix A to paper E/445/16;

(2) delegation to the Director of Finance & Resources in conjunction with the Chief Executive to approve minor changes to the Policy from time to time to reflect system updates/changes;

Members Note:

(3) that any future significant changes will be brought back to Members for approval; and

(4) officers will provide Members with a full update of any changes made to the I.T Usage Policy every three years.

BACKGROUND

1 The I.T Usage Policy (the policy) was created in 2008 and was approved by Members on 25 September 2008 (Paper FA/175/08).

2 The policy applies to everyone who has access to Information Technology (I.T) systems used by Lee Valley Regional Park Authority (the Authority) whether in the work place or at home, whether employee, contractor, volunteer or any other

designated user. The Lee Valley Leisure Trust has adopted the Authority's policy.

3 All users are formally required to acknowledge that they understand and accept responsibility for the security and protection of I.T assets (whether use of I.T systems, mobile phones, I.T equipment, confidentiality of data, or the processing of paper documents), by signing that they have read and understood the policy (this document is held in the I.T office).

4 The purpose of the policy is to define the acceptable use of I.T equipment and related services, systems and facilities by providing clear guidance as to what is, and what is not, acceptable behaviour in the use of I.T systems.

5 The policy is currently reviewed every three years by the I.T Manager or sooner if material changes occur.

6 Members of Executive Committee considered proposed changes to the I.T Usage Policy at its meeting earlier today (paper E/445/16), attached as Annex A to this report, and an oral update will be provided at the meeting.

7 Any environmental, financial, human resource, legal, risk management and equality implications are covered within paper E/445/16.

Author: Simon Sheldon, 01992 709 859, ssheldon@leevalleypark.org.uk

PREVIOUS COMMITTEE REPORTS

Finance & Audit Committee	FA/175/08	Information Technology (I.T) Usage Policy	25 September 2008
Executive Committee	E/445/16	I.T Usage Policy Review	28 April 2016

ANNEX ATTACHED

Annex A	Paper E/445/16

LIST OF ABBREVIATIONS

the policy	I.T Usage Policy
IT	Information Technology
the Authority	Lee Valley Regional Park Authority
the Trust	Lee Valley Leisure Trust (T/a Vibrant Partnerships)

Lee Valley Regional Park Authority	Agenda Item No:
LEE VALLEY REGIONAL PARK AUTHORITY	6
EXECUTIVE COMMITTEE	Report No:
28 APRIL 2016 AT 11:00	E/445/16

I.T USAGE POLICY REVIEW

Presented by the Director of Finance & Resources

EXECUTIVE SUMMARY

The Authority has an I.T Usage Policy which governs how staff use Information Technology. The Authority engages the Lee Valley Leisure Trust as its IT support service and the I.T Usage Policy has now been reviewed and revised to reflect changes in I.T systems, processes and technology within the Authority.

RECOMMENDATIONS

Members Recommend to Authority:

(1) the changes and additions to the I.T Usage Policy set out at Appendix A to this report;

(2) delegation to the Director of Finance & Resources in conjunction with the Chief Executive to approve minor changes to the Policy from time to time to reflect system updates/changes;

Members Note:

(3) that any future significant changes will be brought back to Members for approval; and

(4) officers will provide Members with a full update of any changes made to the I.T Usage Policy every three years.

BACKGROUND

1 The I.T Usage Policy (the policy) was created in 2008 and was approved by Members on 25 September 2008 (Paper FA/175/08).

2 The policy applies to everyone who has access to Information Technology (I.T) systems used by Lee Valley Regional Park Authority (the Authority) whether in the work place or at home, whether employee, contractor, volunteer or any other designated user. The Lee Valley Leisure Trust has adopted the Authority's policy.

3 All users are formally required to acknowledge that they understand and accept responsibility for the security and protection of I.T assets (whether use of I.T systems, mobile phones, I.T equipment, confidentiality of data, or the processing

of paper documents), by signing that they have read and understood the policy (this document is held in the I.T office).

4 The purpose of the policy is to define the acceptable use of I.T equipment and related services, systems and facilities by providing clear guidance as to what is, and what is not, acceptable behaviour in the use of I.T systems.

5 The policy is currently reviewed every three years by the I.T Manager or sooner if material changes occur.

POLICY CHANGES

6 There have been a number of changes and additions to the policy which are as follows:

- Section 3.1 Unauthorised use or removal of I.T equipment
- Section 3.2 Regarding un-authorised devices on the network
- Section 3.6 Regarding probity around passwords
- Section 4 Regarding the use of Wi-Fi *(new section)*
- Section 6.4 Regarding the deletion of old users accounts *(new section)*
- Section 6.7 Regarding the use of the 'Everyone with email' distribution group *(new section)*
- Section 7.1 Regarding remote access
- Section 9.6 Regarding how backups are done
- Section 11 Regarding mobile devices
- Section 11.15 Regarding the misuse of mobile devices *(new section)*
- Section 13.3 Regarding the misuse of hardware *(new section)*
- Section 13.4 Regarding the rolling replacement of hardware
- Declaration Updated wording in declaration

It should be noted that minor changes relating to job titles, responsible officers and terminology have been made throughout the policy.

7 A more detailed description of what these changes are can be found in Appendix A to this report. A full copy of the policy can be found at Appendix B to this report.

8 These changes have been made to reduce the risk of misuse of I.T equipment and systems, make staff more accountable for Authority equipment and to reduce any network security vulnerabilities.

9 The changes that have been made will give relevant officers greater control over the use of Authority I.T equipment and systems.

10 All staff will be required to sign that they have read and understood the revised policy once the changes have been approved by Members.

CONTINUAL REVIEW

11 It is important that the policy remains current and relevant as new amendments relating to changes in technology, systems or security protocols are reflected immediately within the policy. Members are asked to approve delegation to the Director of Finance & Resources in consultation with the Chief Executive to allow these changes to be made as necessary.

12 To ensure that the policy remains up to date, the frequency at which the policy is formally reviewed will be every three years; however due to the nature of technology and how quickly it can change, the frequency at which the policy can be reviewed may happen within the three year period.

APPROVAL PROCESS AND LEGAL

13 In accordance with Standing Orders full Authority is required to approve the policy to ensure that it has effect in the event of a legal challenge.

14 Due to potentially high frequency of changes and the need for their immediate adoption, it is recommended that the process of approving future changes to the I.T Usage Policy be delegated to the Director of Finance & Resources, with the caveat of any significant changes being referred back to Members for approval.

15 For any changes to the policy to be approved they will be taken to the Authority Senior Management Team meeting for discussion before a decision under delegation is taken.

16 To ensure thorough scrutiny of the policy it is recommended that a report summarising any interim changes be reported to Members every three years.

ENVIRONMENTAL IMPLICATIONS

17 There are no environmental implications arising directly from the recommendations in this report.

FINANCIAL IMPLICATIONS

18 There are no financial implications arising directly from the recommendations in this report.

HUMAN RESOURCE IMPLICATIONS

19 Employees will be required to sign their acceptance, understanding and adherence to the I.T Usage Policy through the declaration shown at the end of the Policy.

20 Employees will become more accountable for equipment under the updated Policy.

LEGAL IMPLICATIONS

21 In preparing the Policy on behalf of the Authority, Lee Valley Leisure Trust has ensured that it is compliant with all applicable law.

RISK MANAGEMENT IMPLICATIONS

22 The risks are associated with network security and accountability if the amendments are not approved.

23 There is a risk that if amendments are not approved, the Authority will not be able to use the Policy as a reference at disciplinary hearings if misuse of equipment or technology is identified.

EQUALITY IMPLICATIONS

24 There are no equality implications arising directly from the recommendations in this report.

Author: Simon Clark, 01992 709 893, sclark@leevalleypark.org.uk

PREVIOUS COMMITTEE REPORT

Finance & Audit Committee	FA/175/08	Information Technology (I.T) Usage Policy	25 September 2008

APPENDICES ATTACHED

Appendix A	Changes and additions to the I.T Usage Policy
Appendix B	I.T Usage Policy

LIST OF ABBREVIATIONS

the policy	I.T Usage Policy
IT	Information Technology
the Authority	Lee Valley Regional Park Authority

I.T Usage Policy changes

The following changes have been made to the I.T Usage policy

Section	Description	Explanation	Rationale
3.1	Unauthorised use or removal of I.T equipment	Prevent loss of I.T equipment, especially when staff leave unexpectedly	Staff accountability
3.2	Network Security	The disconnection of un-authorised devices from the network. This will give I.T staff the Authority to disconnect (without notice or explanation) any un-authorised device from the network.	Network Security
3.6	Password Security	Updated to state that all users must change their password regularly. Removes the ability to allow any exceptions to this rule	Network Security
4	Wi-Fi.	New section to cover the use of public and corporate Wi-Fi	Network Security
6.4	Disabled Accounts (Leavers)	Deletion of old users accounts. New section regarding the management of user accounts of staff who have left the Authority.	Network Security
6.7	'Everyone with email' distribution group	Access to the 'Everyone with email' distribution group will be restricted to HR, Comms, SMT and I.T users to prevent staff from sending trivial messages to everyone with email. The Authority's Intranet should be used for non-urgent messages.	Staff accountability
7.1	Remote Working Forms	New staff will not be granted remote access to the network until their probation period has been completed. SMT have the authority to overrule if needed.	Network Security
9.6	Backups	The backup process has been changed from tape backups to virtual backups.	Process change
11	Mobile devices	Use of mobile and tablet devices such as iPads was not covered in the previous policy.	Hardware change
11.15	Mis-use of Mobile device	New section about misuse of mobile devices, allowing the the ability to re-charge the user if persistent loss or damage is discovered.	Staff accountability
13.3	Mis-use of Hardware	New section about misuse of hardware (such as laptops, screens etc) allowing the ability to re-charge the user if persistent loss or damage is discovered.	Staff accountability
13.4	Hardware Replacement	The process of replacing PC's every three years is no longer required or sustainable. Wording that stated PCs will be replaced every 3 years has been replaced with 'Once a piece of hardware has reached the end of its warranty/guarantee term it will either be replaced, refurbished or have the warranty/guarantee extended'.	Efficiencies
Declaration	Declaration	Wording in the declaration has been updated to cover any future updates.	Staff accountability

This page is blank

Lee Valley
Regional Park Authority

I.T Usage Policy

Information Technologies (I.T.)
Lee Valley Regional Park Authority





ITUP

This document is controlled by Lee Valley Regional Park Authority.

Lee Valley Regional Park Authority,
Myddelton House, Bulls Cross,
Enfield, Middlesex, EN2 9HG

Version Control

Updated on	Details	Updated by	Issue No
September 2008	Approved by Members 25/09/08 (Paper FA/175/08)		1.0
October 2013	Circulated to Policy and Procedure Review Group for discussions		1.0
November 2013	Comments from P&P Review Group		1.0
December 2013	Version for Exchange to review		1.0
May 2015	Updated Backup Section	Simon Clark	1.1
09/07/15	Updated Mobile device section	Simon Clark	1.2
18/09/15	Updates following Policy working group meeting	Simon Clark	1.3
26/10/15	Updated with Authority logo and details	Simon Clark	1.4

Lee Valley Regional Park Authority

Document Information

Title: I.T. Usage Policy

Status: Draft

Current Version: v1.4

Author IT Manager
itsupport@leevalleypark.org.uk
☎ (01992) 709893

Sponsor Kulvinder Sihota
Managing Director
ksihota@leevalleypark.org.uk
☎ (01992) 709821

Consultation: Policy & Procedure Review Group

Approved

Approved by: Awaiting Sign off from Management Team
Approval Date: Awaiting Sign off from Management Team

Review Frequency: Every 3 Years
Next Review: January 2018

Contents

INTRODUCTION

This policy applies to everyone who has access to Information Technology (I.T.) systems used by the Lee Valley Regional Park Authority (LVRPA) whether in the work place or at home, whether employee, contractor, volunteer or any other designated user.

All I.T assets are owned by the Lee Valley Regional Park Authority and are loaned to the LVRPA for use in relation to work carried out for the LVRPA and/or the Authority.
All users must understand and accept responsibility for the security and protection of I.T assets (whether use of IT systems, mobile phones, IT equipment, confidentiality of data, or the processing of paper documents), by signing this I.T Usage Policy.

DEFINITIONS

For the purpose of this document, the term 'I.T', 'I.T. equipment' or 'I.T. Systems' will cover; desktop computers, laptops, notebooks, telephones (including mobile phones and iPhones), printers, routers, servers, e-mail accounts and any other associated hardware and software in use both directly or indirectly.

For the purpose of this document, the term 'users' and 'staff' will mean; employees, agency staff, voluntary workers, Authority Members and contractors.
Furthermore, the term 'LVRPA' and 'Authority' will mean the Lee Valley Regional Park Authority.

OVERVIEW

The purpose of this policy is to describe the acceptable use of I.T equipment and related services, systems and facilities by providing clear guidance as to what is, and what is not, acceptable behaviour in the use of I.T. systems..

The Policy is maintained and regulated by LVRPA and is cross-referenced to, and by, a number of other Authority policies and regulations, in particular, the Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000, the Freedom of Information Act 2000 and the Human Rights Act 1998.

Users are reminded that this policy has been written in the context of the basic laws of the land, which have been strengthened over the past few years to cover these areas;

The Managing Director of the Authority is responsible for ensuring that this policy and related procedures are up-to-date, relevant and are adhered to by all users of I.T. equipment within the Authority.

The Policy will be made available to users of any I.T system (email and related services and facilities) and will be reviewed every three years, or before if there is a need i.e. legislation. This will be necessary with regard to the expected development of the system, the operational use of the system and generally recognised best practice.

Email services are provided by the Authority to support its primary role of work and associated functions related to this role.

STATEMENT OF TRUST

This policy is intended to detail the rules of conduct for all users of the Authority who use I.T. equipment. This policy applies to the use of any I.T system, including hardware, software and networks, provided by the Authority. The Policy is applicable to **all** users.

Only authorised users of the Authority are entitled to use its I.T. equipment. All users of the Authority, who agree and abide by the Authority regulations, are able to use computing facilities and email systems at all times when the network is available.

The Authority complies with and adheres to all its current legal responsibilities including Data Protection, Electronic Communication, Regulation of Investigatory Powers (RIP), Human Rights, Computer Misuse, Copyright and Intellectual Property.

1. STATEMENT OF RESPONSIBILITIES

All Managers will be responsible for ensuring their staff are aware of this policy.

Individual users are responsible for their own actions. The use of I.T. equipment by individuals within the Authority assumes and implies compliance with this policy, without exception, and those Acts, Policies and Regulations referenced above and enacted or authorised by the Authority or other regulatory bodies. Every user has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.

I.T. equipment and software should only be used in accordance with this policy and not in any way that will bring the Authority into disrepute.

I.T. equipment should be looked after as if it were the users own property and kept secure when not in use. Only designated users of the Authority are authorised to use Authority equipment. This means it must not be used by either family or friends.

Any loss or damage to the Authority's I.T. equipment must be reported to the I.T. section immediately. Any loss or damage of equipment which is attributable to the negligence or irresponsible use by the user will require that individual to reimburse the Authority for the full replacement cost of that equipment.

The I.T. equipment available is provided for the efficient performance of the Authority's business. Irresponsible use of IT or failure to take reasonable care will become a disciplinary matter.

1.1 I.T department specific responsibilities

The I.T department will perform the following roles and tasks:

- Central purchase of LVRPA I.T equipment on behalf of all LVRPA sections regardless of which budget the equipment is funded from. In accordance with Financial Regulations all I.T equipment purchases must be authorised by the I.T Manager.
- Installation, configuration and maintenance of I.T equipment purchased.
- Maintenance of an accurate register of I.T equipment issued to the user. The user is responsible for returning all I.T and telephony equipment prior to leaving LVRPA in a timely manner.
- The I.T department will provide remote support via telephone and remote access software as required. Home visits will not be made and users will be required to bring their equipment in house for rectification/repair.
- The I.T department will (via Group Policy) control various settings on Authority equipment for security and efficiency reasons. The policy will control such things as the type of printers that are deployed to users, Internet settings, desktop settings (including desktop Icons, desktop backgrounds and screensavers), user rights levels and hardware installation.

GENERAL COMPUTER USAGE

1.2 Acceptable Use of I.T Equipment

Users are reminded that any I.T equipment issued is to allow the user to undertake their work duties and should be considered as work equipment. Any personalisation can be removed by I.T without notice or recompense.

It will be considered unacceptable use if users access, download, upload, post (on websites) or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist, defamatory, libellous, intentionally false or inaccurate or inappropriate. If a user receives such material, they should report the matter to the I.T Manager immediately, who will then contact the relevant line manager to make them aware of the situation. Disciplinary action will be taken against anyone who is found to be sending such material.

It will also be considered unacceptable use if users fail to look after and/or maintain any I.T equipment that is issued to them or if it is used in a way that is not befitting of the item or would be deemed to be inappropriate.

Any perceived intended or intentional damage caused to any I.T equipment will be viewed as unacceptable and will result in access to that equipment being removed completely and any damage paid for.

Failure to comply with the acceptable use of I.T equipment as contained in this policy could result in disciplinary action being taken.

1.3 Login hours

The current permitted login hours for users is between 06:00am and Midnight . This is to allow maintenance and updates to be carried out if needed.

Login hours can be extended if a need is identified (such as an Event that starts early or finishes late). The Line Manager of the user must email I.T giving authorisation for the user to have their login hours extended. Any extensions will be temporary and will be reset once the required period for the extension has expired.

1.4 Housekeeping

Users are also responsible for keeping PC's and associated equipment clean and in good general physical condition. Cleaning materials can be purchased from the Authority's stationery suppliers, the cost of which will be paid for out of individual department budgets.

Food and drink should not be placed on any I.T equipment and users should take care when consuming food and drink when in close proximity to I.T equipment. Food and Drink must not be consumed in any of the venues server rooms.

1.5 Intellectual Property Rights

The ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. Users must not alter or copy a file that iswrite protected (belonging to another user) without first obtaining written permission from the creator of the file.

1.6 Transporting Equipment

When transporting I.T equipment, for example, a laptop in a user's car, it must be stored in the boot of the vehicle and be out of visible sight. The boot of the car must, where possible, be kept locked at all times even when you are driving.

On arrival at the destination the I.T equipment should be removed from the vehicle as far as is practically possible.

1.7 Using Equipment Abroad

I.T equipment including mobile devices should not be taken and used abroad without the prior consent of a Management Team Officer.

If approval is given, the user must inform I.T as user account log in changes may be required, depending on which country is being visited due to the time differences.

Mobile devices must have data roaming and 3G services turned off whilst abroad to prevent excessive network charges and Wi-Fi should be used where possible. Special tariffs can be arranged via the network provider, if data is required when abroad.

1.8 Procurement of Equipment

All I.T equipment (Hardware and Software) must be either purchased by or through the I.T department as it is important that the equipment is added to the I.T department's inventory, security tagged and purchased from approved suppliers.

1.9 Copyright and Downloading

Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded, re-used on the Authority's website or transmitted to third parties.

2. HOURS OF SUPPORT

The I.T Departments normal business hours are from 08.00 to 17.00 Monday to Friday.

I.T Services are usually available during normal business hours, except if system maintenance has been agreed. Support is available at these times.

2.1 How to contact I.T Support

All requests for assistance should first be logged at the Department via one of the following methods:

- Email – Send an email to **itsupport@leevalleypark.org.uk**. Emails should not be sent directly to IT staff unless it is of a sensitive or personal nature.
- On-line portal – Use the on-line portal: **http://itsupport.leevalleypark.org.uk** (a link to the portal has been added to Compass.
- In person - Visiting the IT department in person.
- Phone – Call the IT department either on landline or mobile (phone numbers are listed below).

Post	Ext	mobile
I.T. Helpdesk	808	
I.T. Manager	893	07734 021746
I.T. Support Tech	811	07917 647553
I.T. Support Tech	949	07739 851932

Calls will be categorised as either Incidents or Service Requests (Tasks). In general, resolution of incidents takes precedence over fulfilment of Service Requests (Tasks).

3. SECURITY

All users of I.T equipment should make every effort to keep I.T equipment secure and prevent items being from being able to be stolen or removed without consent. This could mean having to purchase additional equipment such as PC locks to secure equipment, especially where equipment is in public areas.
Doors to offices should be locked when not in use and inventory checks on equipment pre and post events should be undertaken to identify any loss.

3.1 Unauthorised use or removal of I.T equipment

The unauthorised use or removal of I.T equipment is defined as, the using or taking of I.T equipment (includes software licences) without prior approval from a Senior Manager or the I.T Manager.

The unauthorised taking or using of I.T equipment will be deemed as gross miss-conduct.

3.2 Network Security

The I.T department have an obligation to ensure that the Authority network is secure and that there is no un-authorised access to the network. Only Authority issued devices are allowed to connect to the network; which means that external contractors and staff personal devices are not permitted to connect to the network.

If an un-authorised device is detected on the network it will be disconnected (either remotely or physically) by the I.T department without notice or explanation.

Staff should not allow external contractors etc. to connect devices to network points or to the corporate Wi-Fi network.

3.3 Penetration Testing

The I.T department will conduct regular penetration testing on the network to ensure that there are no vulnerabilities and will action any issues that are discovered as soon as they are identified. This may require the network being taken down whilst the work is carried out. Notification of any downtime will be given; however due to the seriousness of the vulnerability the amount of notice may be short if at all.

3.4 Firmware

It is essential for security that the latest versions of firmware are applied to network devices and as such the I.T department will need to apply firmware updates to network switches, servers and other network devices.

In some instances the firmware updates require a reboot of the hardware for the update to apply; which will result in the network being taken down whilst the work is carried out. Notification of any downtime will be given; however due to the importance of the updates the amount of notice may be short if at all.

3.5 Server Updates

The I.T department undertake monthly server maintenance once a month in-line with Microsoft's 'Patch Tuesday'; where the latest security patches are made available by Microsoft.

The updates require the servers to be rebooted which will result in the servers being unavailable whilst the work is carried out. Notification of maintenance will be given in advance; however if an emergency patch is published by Microsoft an immediate reboot of the servers may be required without notice.

3.6 Password Security

Users are responsible for safeguarding their own password for all corporate systems and applications. For reasons of security, individual passwords must not be printed, stored on-line or given to others. Password rights given to users should not give rise to an expectation of privacy.
All passwords should be at least eight characters long and contain upper/lower case Alpha and numeric characters and should not be guessable (e.g. partners name, favourite football team etc.).

All users must change their password at least once every 60 days. Failure to do so will result in the user being automatically locked out of the system.

For mobile telephones a PIN security number must be used to access the phone. The PIN must not be disabled or turned off and the PIN must be difficult to guess i.e. not 1234 etc.

If a user feels that their password has been compromised, it should be changed by the user immediately and reported to the IT manager. Users should contact I.T if they are unsure how to change their password.

3.7 Account lock outs

User accounts are set to lock out after three failed attempts of inputting a password; this is done to prevent un-authorised access to the network. Accounts can only be unlocked by the I.T department.

3.8 Locking PC's

To prevent PC's from being used for unauthorised access and/or sensitive files accessed, they must not be left unattended without being put into a 'locked' state (press 'Ctrl' + 'Alt' + 'Delete' Users should contact I.T if they are unsure how to 'Lock' a PC) or shut down. PC's will automatically 'lock' themselves after 15 minutes of inactivity.

Screensavers should not be used as a substitute for these measures. When using screensaver the 'on resume, password protect' box must be un-ticked

4. WI-FI

4.1 Corporate Wi-Fi

At the majority of the venues there is corporate Wi-Fi available that staff can have access to work on devices for work purposes. The Wi-Fi networks broadcast their SSID's and are suitably protected using WPA2 encryption.

Only Authority approved devices are permitted to be connected to the corporate Wi-Fi networks. Any personal or external devices found on the Wi-Fi network will be disconnected without notice or explanation.

4.2 Public Wi-Fi

At the majority of the venues there is Public Wi-Fi; which at some of the venues offer the service for free (Velo, WhiteWater etc.), whilst some include the costs in agreements (Marinas and Campsite (static home owners)) and some charge (Campsite (touring) and Visitor Centre at Mydd House).

Staff requiring public Wi-Fi on personal devices should connect to the public Wi-Fi.

User data is captured when they sign up and as long as the relevant acceptance box has been ticked their data is added to the Organisations CRM database.

5. RISK ASSESSMENT, AUDITS & MONITORING

The Authority will take steps to reduce any risks associated with the use of I.T.

The major risks faced by the Authority include:

- Damage to its reputation
- Security/integrity of its network
- Careless or frivolous use resulting in damage to equipment
- Loss of confidential data
- Failure to enforce its own policies against discrimination
- Allowing a culture to develop that does not best meet the needs of the business.

To mitigate against such risk, the Authority believes it should monitor directly, activities undertaken by individuals while using IT equipment whether for business or personal use. The methods of monitoring include:

- Regular Internet usage monitoring
- Regular e-mail usage monitoring
- Regular telephone usage monitoring (both landline and mobile)
- Regular equipment audits (announced and unannounced) to check only approved Authority applications and usage.
- Computer monitoring via specialist third party software.

Preventative work will also be applied to ensure that the monitoring identified above is not the sole means the Authority uses to protect against these risks. This includes:

- Using Internet Monitoring software to prevent access to sites the Authority deems unacceptable
- Using "spam" and email filtering to detect and prevent un-solicited e-mails and e-mails of an offensive nature.
- Induction training to ensure all new employees are aware of the policy
- Anti-virus software
- PC audits

The Authority will respect where possible the privacy of individuals within their e-mail usage if that e-mail is marked in the subject line "Private & Confidential". E-mails marked in this way will not normally be opened unless there are exceptional circumstances, for example, where harassment or criminal activity is suspected, or where normal monitoring processes indicate the e-mail contravenes this policy directly, for example through the language used or it may be carrying a virus.

The Authority will not undertake covert monitoring on a routine basis. Covert monitoring will only be used in cases involving suspected criminal activity or malpractice or the apprehension or prosecution of offenders. Such activity would require the authorisation of Senior Management and a note to the justification of such activity made. Monitoring of this nature would only occur in circumstances in which the police would normally be interested and where openness would normally prejudice the investigation.

5.1 Auditing

The Authority reserves the right to audit and/or monitor I.T equipment and usage in any way that it deems appropriate for any piece of I.T equipment owned by the Authority with or without prior notice to the user to ensure that these standards are being complied with.

PC audits will be carried out by I.T staff on a regular basis. Users will be required to immediately surrender their equipment to I.T staff to allow the audit to be carried out.

5.2 Consequences of Violation

Any security breaches that occur must be treated seriously as they may compromise the LVRPA, its systems and network.

In the event of burglary/theft of equipment or data, the employee must report the crime immediately to their local police force (obtain a Crime ref. number) as well as to their Line Manager and to the IT Manager. The employee must also report immediately any security incidents involving/affecting LVRPA equipment, systems or data.

In the event of the employee breaching any of the above procedures or where conduct is considered inappropriate, action may be taken to remove the remote access facility and any equipment provided for that purpose, including computer hardware and software. The removal of facilities may take place with or without notice dependent on the circumstance of the breach and after consultation and agreement by Management Team. Disciplinary and or criminal action may also be taken dependant on the nature and severity of the breach.

6. EMAIL

The Authority's main purpose in providing I.T facilities for email is to support approved business activities of the Authority. I.T facilities provided by the Authority for email should not be abused. An absolute definition of abuse is difficult to achieve and includes (but is not necessarily limited to):

- Creation or transmission of material which brings the Authority into disrepute.
- Creation or transmission of material that is illegal.
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk-mail of any kind
- The unauthorised transmission to a third party of confidential material concerning the activities of the Authority.
- The transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serve to deny service to other users.
- Activities that corrupt or destroy other users' data or disrupt the work of other users.
- Use of Authority email addresses for personal use.
- Use of Authority email addresses for private business use e.g. auction sites.
- Creation or transmission of any offensive, obscene or indecent images, data or other material.
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, and disability, political or religious beliefs.
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature.
- Activities that violate the privacy of others or unfairly criticise, or misrepresent others; this includes copying distribution to other individuals.
- Creation or transmission of anonymous messages or deliberately forging messages or email header information, (i.e. without clear identification of the sender).
- The deliberate unauthorised access to services and facilities.
- The unauthorised provision of access to Authority services and facilities by third parties.

6.1 Personal use

Personal use of Authority email addresses is not permitted and as such should not be used as a primary email address for such things as social networking sites, on-line subscriptions or e-commerce sites etc.

6.2 Quotas and limits

All users have access to the centrally-managed email server. All accounts have quota limits placed on them, which if exceeded will result in the email account being disabled. Quotas are set to ensure fair usage and to ensure servers do not become full.

Users receive an email notification when approaching their quota limit and are required to follow guidance in this email to manage their account. The final email that is received which takes an individual over their limit will always be delivered. Once over quota no further emails can be delivered to an individual's inbox until they have reduced their storage below this limit. Any email that fails to be delivered because a user is over quota will immediately be returned to the sender.

There are limits on the size of an email that can be received and transmitted. No email greater than 10 Mbytes can be accepted for delivery to a LVRPA account (i.e. inbound). No email greater than 10 Mbytes can be accepted for transmission by the email servers (i.e. outbound).

Users should avoid sending large and/or trivial messages or unnecessarily copying e-mails and Compass should be used to save files that need to be shared and then a link be inserted within the e-mail.

6.3 Archive e-mails (.PST)

Users should keep mailboxes to a minimum by regularly deleting old and irrelevant e-mails; however where there are circumstances where e-mails need to be kept, an archive folder can be created to store them in.

Archive folders should be managed in the same way that the mailbox is managed by regularly deleting old and irrelevant e-mails. We recommend that the archive folder should not exceed 2GB in size as this may cause the folder to become corrupt and fail to open, resulting in a total loss of any e-mails saved in the folder.

Archive folders can be set up on the server (although this is not recommended by Microsoft) as the folders will then be automatically backed up or they can be set up locally on the PC's hard drive, where they will have to be backed up by the user. A limit of five Archive folders per user is permitted to be saved on the server.

6.4 Disabled Accounts (leavers)

When a user leaves the employment of the Authority the account will be disabled and the password reset at 5pm on the day that they are due to leave.

After a period of 30 days the account will be everyoneed and all emails will be irrecoverable. A request from a Senior Manager will be required if an account is required to be kept longer than 30 days.

6.5 Email Virus checking

One common method of distributing malware is via email. All email communication through the LVRPA email gateways is checked for malware; however this should not be solely relied upon and users have a

responsibility to be diligent and to not open e-mails or attachments that appear suspicious. Users should contact I.T if they have any doubts as to the integrity of an email.

The current policy is set to refuse messages containing executable attachments and ZIP files as these pose the biggest security risk. I.T department should be contacted if .Zip files need to be received.

Users must contact I.T immediately if a suspicious attachment is opened so that if there is a threat to the system it can be addressed straight away.

6.6 Email addresses and distribution group lists

All members of staff will be allocated an email address based on their initials and surname. Email address duplications are not allowed, so it is sometimes not possible to offer the exact email address to users. Specific email addresses can be requested for individual or group use if there is legitimate requirement. Email addresses will not be changed for arbitrary or trivial reasons and the final decision on whether a reason is valid lies with The I.T. Manager.

An Email address will not be created without the relevant authorised forms and accounts will remain disabled until the I.T usage policy declaration is signed and returned to I.T.

Email distribution group lists can also be created centrally by the I.T. department. Individuals will need to complete a Distribution Group form which can be found on Compass. This must be authorised by the Head of Department, then emailed to the I.T. Manager for completion. The distribution groups will be reviewed annually for relevance and if no longer required will be either edited or removed. Staff should make I.T. aware if a distribution group is no longer required.

6.7 Everyone with Email

The only staff who will have access to and therefore are permitted to use the 'Everyone with Email distribution group' email are PR/Comms, I.T staff, Heads of Service, Directors and the Chief Executive. All other Staff will not have access to the 'Everyone with Email' distribution group and must not manually add every individual email address to an email to bypass the system.

Only important news or noteworthy items will be sent using the 'Everyone with Email' distribution group; other news items should be posted on Compass or communicated via the PR/Comms department. Sending trivial information via the 'Everyone with Email' distribution group will be deemed as a contravention of the I.T usage policy.

6.8 Automatic email forwarding

Automatic forwarding or redirection of email to other mail domains is possible, for example the H&S for the LVRPA is contracted out and so emails are set to be automatically forwarded to their mail domain. The I.T. department absolve all responsibility for email forwarded from the network.

It will be the I.T. Department's responsibility to set forwarding up, but it is the user's responsibility to make sure the forwarding address is correct and the email service being used is reputable and reliable. Users must exercise caution when automatically forwarding any email to an outside network and question the need to even do so.

Automatic forwarding or redirection of email within the LVRPA mail domain is not allowed without the consent of a Senior Manager. Allowing other people to access email can be achieved directly by sharing email folders and mailboxes.

6.9 Logging

Traffic through the LVRPA email gateways is logged. Logs include details of the flow of email but not the email content. Transaction logs are kept online for 30 days. Logs are available to authorised systems personnel for diagnostic and accounting reasons.

6.10 Spam and junk mail

Spam can be defined as "the mass electronic distribution of unsolicited email to individual email accounts". Junk mail is usually a result of spamming. In reality spam and junk mail are regarded as interlinked problems.

A certain amount of junk mail is blocked at the mail gateways by our external email filtering provider. Any mail reaching the email gateway which has been marked by these services will be rejected.

Incoming email is also checked by our external email filtering provider and if successfully matched as Spam or junk will be blocked.

The Authority's email system must not be used to send jokes or chain letters and must not be used to Spam other people or organisations.

6.11 Remote access to Emails

Remote access to Authority Exchange email servers is possible via the Internet using Outlook Web Access (OWA) and on mobile devices using 'Activesync' or Exchange on iOS. Please see section on - Remote Working for further information about remote access.

6.12 Emails that discriminate

Users must not make derogatory remarks in e-mails about any other individuals, or groups of individuals including employees, customers and contractors. Any written derogatory remark may constitute libel and may have to be presented in requests under the Data Protection Act 1998.

Any emails that discriminate against employees by virtue of any protected classification including race, gender, nationality, religion, and so forth, will be dealt with according to the Equal opportunities and harassment policy.

If e-mails are received that may be considered to contain derogatory, defamatory, obscene, unlawful, racist, abusive or sexist material, you should inform your Manager, HR Department and the I.T. Manager immediately and such e-mails must not be forwarded to anybody else, unless requested by the above.

6.13 Email format

Always draft e-mails with care and check recipients carefully before sending. Due to the informal nature of e-mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from the computer.

All e-mail must be typed using the approved Arial font.

6.14 Signatures

E-mail signatures are controlled centrally and will consist of your name, job title, direct line and your work mobile phone number (if applicable) and the name and address of your facility / office where you can be contacted by letter.

'your name' – 'your job title'
Direct Line: 01992 709XXX Mobile: 07715 XXXXXX

Lee Valley Leisure Trust
Myddelton House, Bulls Cross, Enfield, Middlesex EN2 9HG
Telephone: 01992 717711 Fax: 01992 719937

The signature will be applied once the email has been sent. This means that the signature will not appear in the email when being created.

Any changes to the standard format must be approved by PR/Comms before being applied and any changes to job titles must be approved by HR before being applied.

Business e-mails sent outside the Authority will automatically be appended with the Authority's standard notice, which currently states:-

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom it is addressed. If you are not the intended recipient, the use of the information by disclosure, copying or distribution is prohibited and may be unlawful. If you have received this email in error please notify the Systems Manager at postmaster@leevalleypark.org.uk. The email should then be deleted.
The views expressed in this message are personal and not necessarily those of Lee Valley Leisure Trust unless explicitly stated."

6.15 Send / Read receipts

Sent and Read receipts should be turned off by default and used only for exceptional e-mails that are sent with high importance.

NB: It is not always possible to receive sent or read receipts if e-mails are sent to an external e-mail address. If a confirmation is imperative it is advisable to telephone to confirm receipt of the e-mail.

6.16 Privacy

There should be no expectation of privacy in any e-mail sent or received. The Authority has the right to monitor any and all aspects of the computer system, including user e-mails to ensure compliance with this policy.

By sending e-mails on the Authority's system you are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the Authority to process such data you should communicate it by other means. It is inappropriate use of e-mail for employees to download, transmit or forward any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory. No user may use the email in a manner that could bring the Authority into disrepute.

7. REMOTE WORKING

Remote working shall be defined as:

"Permanent full-time, part-time or periodic work carried out by employees from a non LVRPA location where network access must be obtained by use of ADSL broadband or 3G card via a Sonicwall VPN client connection. Remote working also includes scenarios where no network access is required."

It can be further classified into the following types of remote working:

- Mobile remote network access using a 3G dongle
- Mobile remote email access via smart phones using Exchange
- Outlook Web Access via non LVRPA equipment either at home or from a non LVRPA PC
- Fixed remote access from home using LVRPA provided equipment
- Out of office LVRPA work using IT equipment which does not require network access
- Mobile remote network access using an ADSL internet connection.

As a general requirement, remote workers must use LVRPA supplied equipment. However, there will be some limited and exceptional circumstances in which remote working can be carried out using personally owned IT equipment. Sensitive or confidential LVRPA work should never be carried out on personally owned IT equipment. The guidance and rules are clearly defined in the section entitled - Acceptable Use of Personally owned IT equipment.

Remote working from abroad using LVRPA laptops is not allowed, unless specifically authorised by a member of the Senior Management Team.

7.1 Remote Working Forms

Users must have successfully completed their probation before being permitted to be setup for remote working (unless authorised by a Director to be setup earlier). Once the probation period has been surpassed users must read and complete a working from home form; which should be submitted through the line manager to the HR Department for verification. Remote access to the IT network will only be set up after the relevant authorisation and risk assessment forms have been correctly completed and received.

On receipt and verification of the above documents the HR and H&S sections will inform the IT department via email that the user can now be set up for remote access to LVRPA systems.

The IT department will set the user up for remote access and inform the Line Manager once completed. This will involve the installation of remote access software on to LVRPA equipment.

7.2 Physical Security

Where possible, the working area set aside for remote working from home, should be a defined separate room to minimise risk and control unexpected interruptions from family and visitors. A lockable cupboard should be set aside to store LVRPA equipment when not in use.

It should be borne in mind that other users of the remote location may not share the user's understanding of the need for discretion.

Physical security must be considered at all times especially the need to protect against theft of LVRPA data and equipment when left in cars, other forms of transport, hotel rooms, conference centres and meeting places.

LVRPA provided I.T equipment is covered under the general insurance for LVRPA equipment; however the excess is such that small claims will not be made and thus replacements may have to be funded from department budgets.

7.3 Equipment and Technical Requirements

The Lee Valley Regional Park Authority owns the I.T equipment and therefore reserves the right to check the equipment and its use at any time as well as to withdraw access where necessary. Checks will be carried out by the I.T section staff on behalf of the Lee Valley Park Authority.

To set up a user to be able to work remotely they will need to have the following:

- A broadband/ADSL connection or a LVRPA 3G dongle.
- Broadband account details (if own broadband)
- A VPN account set up by the IT department on LVRPA Sonicwall.
- Sonicwall client VPN software installed and set up on the user's laptop.

All I.T equipment must be retuned when an employee leaves the employment of the Authority. Failure to return equipment will result in monies, equal to the cost of replacing the equipment will be deducted from any final salary payments.

7.4 Line Managers' Responsibilities

It is the Line Managers responsibility to:

- liaise with HR and H&S for guidance on lone/remote working issues.
- notify HR and H&S via completion of relevant forms in section 7 above of the request to work remotely or from home.
- ensure staff are aware of, and comply with, all relevant LVRPA policies as well as acceptable and prohibited usage of LVRPA information systems, in order to deter any misuse.
- continue normal line management responsibilities and agree terms with the remote worker and HR.
- ensure all issued IT equipment as listed on the IT Asset database are returned in a timely manner when staff are no longer working remotely or are leaving the LVRPA.

7.5 Remote Workers' Responsibilities

- Users must comply with the full requirements of this policy, including:
- Taking personal and sole responsibility for protecting LVRPA assets and data entrusted to their safe keeping.
- Have the facility to securely lock away all IT equipment when not in use.
- Only use the LVRPA IT equipment for official and authorised purposes.
- Log off IT equipment when unattended, particularly when connected to the LVRPA network.
- Do not advertise that you are working on LVRPA information at home or when working remotely.
- Report any IT equipment faults or failure immediately to the IT department and do not allow any non LVRPA IT personnel access to the equipment for repair. The equipment should be returned to the IT department for rectification/repair.

8. ONLINE USAGE

User's responsibilities when engaging in on-line activities:

- Users should not engage in activities on the Internet which might bring the LVRPA into disrepute;
- Users should act in a transparent manner when altering online sources of information;
- Users should not use the Internet in any way to attack or abuse colleagues;
- Users should not post derogatory or offensive comments on the Internet.
- Users should not give away or discuss LVRPA confidential information.

8.1 Website

The Authority has its own website which is hosted by an external website development company, but is updated by Authority staff via a content management system (CMS).

Only approved users have access to the CMS and are able to make changes to the website. To become an approved user of the CMS a 'Website Content Management System Access Request Form' must be completed and returned to the I.T Manager.

The website is provided by the Authority and therefore the same rules apply with regards to acceptable use as defined in the 'Acceptable use of I.T' section in this policy.

8.2 Social Media & Blogs

The Authority has set up a number of (approved) official social media accounts (e.g. Facebook, Twitter etc) that are managed by approved users of the Authority.

The use of social media websites on behalf of the Authority is governed by the same rules with regards to acceptable use as defined in the 'Acceptable use of I.T' section in this policy.

Users should not use their own personal social media accounts/sites/blogs to express their personal views or opinions about the Authority or other employees of the Authority, nor should they portray the account as being an official Authority social media account.

All users should adhere to all HR policies and procedures and follow the Social Media Guidelines when communicating using social media. It is the responsibility of marketing and communications team to ensure that social media for LVRPA is monitored and controlled.

In the event of a user breaching any of the above procedures or where conduct is considered inappropriate, disciplinary and or criminal action may be taken dependant on the nature and severity of the breach.

8.3 File Sharing Applications

The use of file sharing applications such as Dropbox, OneDrive and Yousendit are permitted; however users should be vigilant when opening files sent via these types of applications and should only open attachments from trusted sources.

File Sharing Applications are constantly polling the network for new items; which consumes bandwidth and could cause the network to slow down for other users; therefore these applications must be closed (taken offline) when not in use.

8.4 Internet Usage

The provision of Internet access is primarily for Authority business purposes. Users are required to keep access of the Internet to a minimum and to close all internet applications when direct use of them has finished and not keep browser windows minimised at the bottom of the screen.

Minimal private use of the Internet is permitted but must not interfere with work. A reasonable level of personal internet usage is permitted but would not normally exceed a maximum of five hours per week, which is equivalent to an hour at lunch time. A user may request from their manager to use the internet for longer, out of hours, providing they specify when and for what purpose they intend to use the internet for. This would be granted at the manager's discretion.

8.5 Website Monitoring and filtering

Internet usage is monitored centrally on a monthly basis and reported to the Senior Management for each department where potential overuse or misuse is detected.

The Authority uses software to block malicious and undesirable websites and also for scanning web content for threats. Web control policy provides additional security and other filtering options. Access to certain websites deemed unsuitable will be automatically blocked by the web filtering software this includes sites that contain explicit material, streaming video etc. However some sites that contravene the I.T. Usage Policy may still be reachable. Users are reminded that accessing such sites remains unacceptable and will result in disciplinary action.

The following categories are blocked:

Productivity-related categories:
- Gambling
- Games
- Religion

Adult and potentially inappropriate categories:
- Adult/Sexually Explicit
- Alcohol & Tobacco
- Criminal Activity
- Hacking
- Illegal Drugs
- Intimate Apparel & Swimwear
- Intolerance & Hate
- Proxies & Translators
- Sex Education
- Tasteless & Offensive
- Violence
- Weapons

Social Networking:
- Chat

Categories likely to cause excessive bandwidth usage:
- Peer to Peer
- Ringtones/Mobile Phone Downloads

If staff try to access a website that is blocked they will be alerted and will not be able to gain access to that website. The I.T department will be able to see what blocked website a user has been trying to access.

In some instances a website may be blocked; but is a legitimately safe website. In these instances a request can be made to the I.T department to unblock the website (this will not guarantee the site will be unblocked).

If a website is deemed to be safe and does not contravene the policy, the site will be unblocked. If the website does contravene the policy, then Senior Management authorisation must be sought by the user to unblock the website.

8.6 Appropriate Use

It is considered inappropriate to use the Internet to access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory; such material may also be contained in jokes sent by e-mail. Users must not use the Internet in a manner that could bring the Authority into disrepute.

8.7 Downloading Software from Internet

Users must not download or install **ANY** software from the Internet without the prior written approval of the I.T. Manager.

Some software (such as Adobe and Java) prompts for updates of software. Where this occurs, users should contact I.T for verification that the update is safe to proceed with as some updates may impact on other software/systems and may also bundle in unwanted third party software and toolbars.

8.8 Downloading materials from Internet

Users must not download, store on Authority devices or use copyrighted material from the internet (or any other source) without obtaining the prior explicit consent from the copyright holder.

8.9 Streaming

There are times when it is necessary to stream audio or video from the internet for work purposes. In these cases it is acceptable to stream such media; however it is not acceptable to stream music / radio or video / TV for non-work purposes as this takes up bandwidth that will result in a degradation of the whole network for other users.

8.10 Internet Security

Users are advised to be aware of the security risks to the Authority from internet access and to be cautious and exercise common sense when browsing websites.

All private financial transactions, including credit card transactions are at the users own risk. The Authority does not guarantee the security or integrity of such transactions and will not be liable for any loss, financial or otherwise, incurred by a user for a private transaction.

The Internet must not be used for personal profit or in connection with any business interest users may have outside this Authority

9. VIRUSES

Computer viruses are defined as, trojan horses, worms, spyware, malware, ransomware and scareware.

IF YOU DISCOVER A VIRUS ON YOUR PC DISCONNECT IT FROM THE NETWORK IMMEDIATELY AND CALL I.T

The Authority uses Anti-virus software as a first line of defence to combat viruses on the network and PC's. The Anti-virus software will automatically update itself during the day and it is important that you inform I.T immediately if the update fails or shows as disabled (a notification will be displayed on the screen if this occurs).
Users must never attempt to disable or uninstall the Anti-virus software.

9.1 Attachments

To minimise the risks from computer viruses **NEVER** open any attachments with a filename ending in .exe .vbs .com .scr .bat. .Zip or .pif's. If you are unsure about the attachments in an e-mail, call I.T. first before opening them.
Zip files are must be scanned before opening and should never be opened if sent from an unknown source.

9.2 Hoax E-Mails

Do not forward on virus warnings to everyone, no matter how the warning is worded. Many are hoaxes and they can in themselves clog up the e-mail system. Simply forward a single copy to .I.T.

9.3 USB Drives / Removable Media

Removable media such as USB drives must be checked and scanned for viruses by I.T before being used, especially if it has been sent from an external person or company.

9.4 Software

All new software must be scanned for viruses, spyware and malware prior to installation. Users must **NEVER** install unauthorised software of any kind without seeking the prior approval of the I.T. Manager. This includes any form of trial software. The installation of joke programmes, screen savers, electronic Christmas cards, e-grams etc. is not permitted

9.5 Virus Discovery

If you discover a virus on your computer you must do the following:
9.5.1.1 Cease using your PC
9.5.1.2 Disconnect the PC from the network (remove network cable)
9.5.1.3 Contact I.T.

If you have any further questions regarding viruses please contact I.T.

DISASTER RECOVERY

9.6 Backups

Backups of the I.T system are undertaken on a daily basis by the I.T department, using third party software called Shadow Protect. The backups are carried out throughout the day at varying intervals (dependant on the Server).

Data is backed up to a server; which is replicated to a secondary server at a remote location.

If a user requires a file or folder restored from a backup, a request must be made in writing to I.T, detailing what the file is called, when it was deleted, where it was saved and the type of file.

The I.T department will make best endeavours to recover data but cannot guarantee that it can be recovered.

9.7 Server Recovery

There is a Data Backup Services Agreement between Lee Valley Park Authority and iQual Ltd in place; which in the event of a disaster which results in the need to perform a full or partial recovery of data or system; iqual will provide assistance with the recovery. This means that there is a mechanism in place to ensure business critical systems can be restored as quickly as possible; allowing the Authority to get back to business as usual.

One of the Trusts audit requirements is to perform a quarterly test of server recovery from the backups. This means that every quarter, four of the servers will be tested to ensure that they can be recovered in the event of a disaster; this will mean that the servers will be unavailable whilst the test is carried out. The dates of the tests will be published before they take place.

10. DATA STORAGE

10.1 Servers

The Authority has on-site File Servers for the storage of work related data (documents, photos and Videos) only. At present there are no quotas on server storage; however if a user is found to have an excessive number of files saved on the server or if they have personal data saved they will be asked to delete files. Data may be removed without notice if found to be causing problems with space on the server(s).

The Files serves house shared folders and home drives that staff with the relevant permissions can access.

10.2 Shared Folders

Shared folders are folders that allow multiple users to access, but have permissions applied to prevent unauthorised access.

If a single document has been created to be shared within the LVRPA, it should be saved to Compass rather than being stored in a shared drive. This will prevent duplicate documents being saved on the server.

Shared folders will be 'owned' by a senior manager and permissions are typically assigned based on job role or the requirements of owner of the folder.

Access to shared folders has to be made via a 'Shared and home drive access request' form, which must be authorised by the folder owner before I.T will action the request.

10.3 Home Drives

Users can be allocated space on the Authority's server (normally called Z: drive) to store documents and files related to Authority business only. The space on these servers is not limitless and therefore users need to be frugal with what they save on them.

Requests for Home Drives are made when a user starts employment with the Authority. If a Home Drive is required at a later date, the users line manager must submit the request via a 'Shared and home drive access request' form.

Documents and files pertaining to work should always be saved to the server and not on the local drive (normally the C: drive) of the PC.

All documents and files should be regularly reviewed to ensure that they are relevant and still required. Any document that is no longer required should be permanently deleted from the system to free up available storage space and to comply with the Authority's data storage policies.

10.4 Personal Files

Users must not store or save any personal files, documents, music, videos or pictures on to any LVRPA owned equipment.
I.T staff will remove any personal files found on LVRPA equipment without warning or consent.

10.5 USB Drives / Removable Media

All USB Flash Drives/Portable Hard Drives/Data disks used for copying and transferring confidential/sensitive data should have hardware based file encryption installed on it. The use of

encrypted USB flash drives/portable hard drives helps to ensure confidential data remains secure in the event of loss or theft.

USB Flash drives/Portable Hard Drives/Data disks should:

- only be used for transferring data between devices and then the data removed
- not be used as an alternative to permanently back up data.

10.6 Archived Data

All removable storage devices (Flash drives/portable hard drives/ CD's/ DVD's/USB Flash drives) containing any confidential or sensitive data, that has been archived should be stored in a locked cupboard or safe when not in use.

It is the responsibility of all user to ensure that confidential and/or sensitive data and information is held securely and is not moved off-site (i.e. from any of the Authority's main operational buildings) without the prior and explicit approval of your line manager.

11. TELEPHONE / MOBILE DEVICES

For the purpose of this document, any phones (whether land lines or mobiles) issued by the Authority are covered by this policy. Mobile Devices are classed as any mobile communication device, which includes basic mobile phones (for making and receiving calls), smart phones (with Microsoft for exchange enabled device that can send and receive e-mails, synchronise calendars and contacts in real time), mobile internet devices such as 3G dongles and tablets such as Apple iPads.

Mobile devices are issued for the use of work and as such should not be deemed as a personal device. Users of mobile devices must be aware that any communication sent via a Authority mobile devices (whether it be business of personal) is bound by the same rules apply with regards to acceptable use as defined in the 'Acceptable use of I.T' section in this policy, this includes the sending of messages via any message sending application on the device i.e. email, text message, instant messaging etc.

11.1 Acceptable use

The Authority issues mobile devices to staff so that they can perform their duties more safely, effectively and be able to communicate with fellow staff and customers.
They are also an essential health and safety requirement for some staff, especially for those who work alone.
Mobile devices are provided by the Authority and therefore the same rules apply with regards to acceptable use as defined in the 'Acceptable use of I.T' section in this policy.

Under no circumstances are Apple devices allowed to be 'Jail braked'. The act of 'Jail braking' a device will be considered as gross misconduct. .

Mobile devices can be used for making personal calls; however users must declare the cost of personal calls on mobile devices, via Vision each month.

There is a data cap if 1GB per month on the bandwidth on devices that have 3G/4G functionality. The charges for exceeding the cap are excessive and as such users should try to avoid going over the cap.

11.2 Mobile Device Management (MDM)

The I.T department uses MDM software to manage its mobile devices. This software allows the I.T department to configure the devices in-line with security policies.
The MDM software allows for the remote control and tracking of the devices, so that in the event that a device is lost or stolen the device can be tracked and if required wiped of any Authority data. By

accepting a mobile device, users accept that the device can be tracked and wiped without notice if it suspected that there is miss-use or theft of the device.

11.3 Transferring of phone numbers

Mobile phone numbers can be ported to or from our network provider. If a number is to be ported in or out, a Senior Manager must give authorisation before it can be processed.

For numbers that are to be ported away from the Authority a PAC code will be requested and must be used within 10 working days. If it is not used a penalty charge will be applied; which the user will be required to pay themselves.

11.4 Call Forwarding

Call forwarding is available on all phones, however users should be aware that the cost of the forwarded call will be charged to the users bill. Therefore, in order to keep the cost of the bills down, the call forwarding function should only be used in moderation.

11.5 Using phones abroad

Using mobile/smart phones abroad will result in additional charges being applied to when making and receiving calls and texts and for using mobile data.

Mobile/smart phones should not be taken and used abroad without the consent of a user's Line Manager.

If approval is given, the user must inform I.T so that the service provider can be informed and a bill of tariffs obtained.

11.6 Mobile Phone Contract

The Authority currently has a contract with Vodafone and is on the Vodafone Government Saver tariff; which gives the Authority a low monthly line rental commitment and reduced calling costs. Other advantages of the tariff are:

- Simple, good value flat rates for any calls
- Discounted international and roaming charges*
- Spend Manager** – allows us to separate work calls and texts from personal ones
- £50 equipment credit per connection

11.7 Call Charges

Call charges have been significantly reduced under the new Vodafone Government tariff.

All work relates call charges (includes text's and internet use) are paid out of the staff's own department budget cost centre.

All personal call charges (includes text's and internet use) have to be declared and paid for by the user.

International and premium rate numbers are blocked from being dialled by default. If a user needs to be able to make international or premium rate number calls they must get written permission from a Head of Service before this is activated.

11.8 Payment of Phone Bills

The payment of phone bills will be made centrally by the Finance section upon receipt of the bill from Vodafone.
Each device will be recharged centrally to the appropriate cost centre.

Every member of staff who has a mobile device will be issued with a copy of their phone bill, which details all calls made and any text's sent in that calendar month.

It is then the staff's responsibility to check the phone bill and declare any personal usage i.e. calls, text's or internet use. The total cost of personal use must be recorded on Vision, even if there has been no personal usage (a 'nil value' must be recorded) and submitted to Finance who will make arrangements for that amount to be deducted from their monthly salary.

It will be the responsibility of each manager to check that the phone has been used appropriately by their staff following receipt of the detailed monthly bill.

Any dispute as to the correctness of the bill must be discussed directly with Vodafone by the user of the phone.

11.9 New Connections

A Mobile Device Request Form must be completed and approved by a Venue / Line Manager. The flow chart in Appendix A shows the process for requesting a new connection.

Venue / Line Managers will be responsible for deciding who requires a Mobile phone, based on their needs to perform the role safely and effectively.

All new connections are free; however the cost of a new device for the new connection is **chargeable** and will be paid for out of the **department's own budget**.

All mobile devices can only be ordered by the I.T Department. Staff are not permitted to order their own mobile devices.

11.10 Mobile Device Options

The Authority offers a smart phone (currently an Apple iPhone) for users who require e-mails on the device and a standard mobile phone (currently Nokia) for users who do not need e-mail on the device. The individual need of the user will determine the type of device issued.

3G and 4G dongles are available for users who need to have internet access on a laptop when not in the office.

The prices are constantly being changed by Vodafone as new models are released; therefore prices are published on Compass.

11.11 Upgrading (Mobile Phone)

The annual free upgrading of mobile device option is now no longer available. Previously staff were automatically offered an upgrade on their mobile device every 12 months.

The credits gained for each connection will be combined to create a central pot of money, of which a proportionate amount will be used to discount the price of a new device, until the money has run out.

All upgrades must be authorised by the line Manager of the member of staff requesting the upgrade. Upgrades will not be carried out if a user just wants the latest device or if the current device is working fine and meets the need of the business. The user or line manager must state the reason for the upgrade on the Mobile Device Request Form.

Upgrades should only be carried out if the device no longer meets the needs of the user i.e. the user changes jobs, or if the phone does not function properly (and is no longer in warranty).

Due to the type of contract the Authority is on, we no longer get 'free' upgrades after 12 months, instead we have two price brackets 'S' and 'U'.

'S' costs relate to new connections or replacement phones that have not already been replaced since the new tariff started.
If a phone is replaced during the two year period of the Government Saver Tariff then the handset will be charged at the 'U' cost.

11.12 Upgrading (Services)

All phones by default are automatically put on the government saver tariff without WAP (internet) service.

The type of device being used will dictate whether or not the WAP service is required i.e. an iPhone will automatically have WAP service enabled.

Adding services such as WAP will increase the monthly charge (see Tariff & Charges table) and as such must be considered if upgrading the device.

11.13 Upgrading (Software)

Certain phones / devices require software upgrades either for the phone or for the PC. Examples of this are versions of Active Sync and iTunes for the PC and iPhone OS (iOS) for the phones.

Upgrading software is one of the stages of resolving issues with phones. Staff should not download and install any upgrades unless told not to do so by the I.T Dept. This is to prevent any device bugs or glitches affecting the user from working on their mobile.

11.14 Re-distribution

All Mobile devices must be returned to the I.T department by the user when they leave the employment of the Authority or if it is decided that they are no longer required. This includes any peripherals that may also have been purchased i.e. in-car chargers, hands free kits, memory cards and covers.

The returned devices will then be wiped, reset to factory settings and held centrally and re-issued to new staff or issued as a replacement for any lost or damaged devices. Any data on the device will NOT be backed up before the device is wiped; therefore **users should ensure that all personal data is retrieved from the device before returning it!**

When a device that has been returned by someone who has left the Authority is available then this can be issued as a replacement (as long as it fits in with their category type).

As and when a device becomes too old to be re-issued it will be removed from circulation and disposed of at an approved re-cycling centre.

11.15 Mis-use of Mobile devices

Mobile devices can be costly pieces of equipment and as such Staff should take steps to ensure that they are kept secure and are not damaged; this may include purchasing protective cases and not leaving the phone unattended at any time.

Miss-use of mobile devices will be construed as:

- Leaving a phone un-attended, which results in the device being lost or stolen
- Making calls to premium rate numbers
- Excessively high call charges
- Calling phone services such as the speaking clock and 118 directory services
- Using the device for purposes other than what it is designed for
- Persistent damage i.e. repeatedly breaking screens etc.

If miss-use of mobile devices is identified the user will be charged the cost of the repair or replacement of the device.

11.16 Damaged or Lost Mobile Devices

Faulty devices

If a device develops a fault, it will be the responsibility of the user to report it to I.T department. If it cannot be fixed by I.T it will be reported to Vodafone as a fault.

If the device is still under the warranty (within 1 year for the old tariff & 2 years for the new tariff) Vodafone will replace it with a like for like device free of charge (Unless it is proved to be due to negligence by the user).
If the device is not under warranty a fee will be charged by Vodafone (Fees vary depending on the device), which must be paid from the users own budget.

Damaged devices

If the device is damaged as a result of work, for example if the phone was on a member of staff who had to enter water to rescue a member of the public, then the repair costs can be paid by the centre. If the damage was caused to negligence or by a friend or family member who had been using the device then the costs for repair will have to be borne by the user.

Damaged devices must be repaired in the first instance – Having a damaged device does not entitle a user to get a newer or different device. If the device cannot be repaired an equivalent or older device will be issued in its place.

Lost or stolen Devices

If a device is lost or stolen the user must report it to Vodafone immediately, so that the 'Sim' card can be blocked. Failure to report a lost or stolen device immediately could result in the user being charged for any charges incurred, including calls made after the phone was lost and the cost of replacing the device.

Vodafone: 0333 304 3333

If a device is stolen, the user must also report it to the police and obtain a crime reference number and the I.T department must also be informed so that records can be updated, before a new device can be purchased.

The cost to replace lost or stolen phones will be charged to the staff's departments budget cost centre or to the member of staff directly, if deemed necessary.

Spare devices

There are generally spare devices held centrally which may be issued as an interim to staff if their phone becomes damaged or is lost. The maximum time that a spare device can be issued is two weeks.

Constant loss or abuse of mobile devices will be investigated and if deemed appropriate the use of a mobile device may be rescinded or the type of device issued downgraded to a lower spec.

11.17 Activations & Locked Devices

When a new device is purchased, the 'Sim' card in the device will need to be activated before it can be used. This can be done by I.T or the Finance & Resources Management Support Officer.

If a device becomes 'locked' i.e. the 'Sim' card is locked due to wrong password being entered, then the user must contact Vodafone for a reset code.

Vodafone: 0333 304 3333

11.18 Peripherals

Peripherals for devices such as in-car chargers, memory cards and covers will have to be purchased from the users own budget on approval of their line Manager. All orders of this kind must be done by the users department.

Being a Authority customer we are entitled to 30% off the list price for accessories when bought through Vodafone.

11.19 Mobile Apps

The use of 'Apps' on mobile devices is permitted on Authority mobile devices as long as do not contravene any rule as defined in this policy. Apps should be purchased under the users own account (iTunes or Android store) and if required for work, the fee be reclaimed via an expenses claim form.

11.20 Hands free kits

Staff should not use mobile devices when driving, therefore the use of hands free kits is not permitted when on Authority business. Hands free kits should not be purchased by the Authority.

12. PERSONAL EQUIPMENT

12.1 Personally owned computers

It is considered acceptable for staff to carry out LVRPA work on their personally owned computers for occasional out of hours work; however staff must have followed the 'Working from home procedure'.

When using personal equipment for work general data should be stored and transported on encrypted USB flash drives provided by LVRPA and funded from individual department budgets.

Confidential or sensitive LVRPA data should never be stored on any portable drive/equipment and never worked on using personally owned computers. This type of data should always be stored and saved to LVRPA servers. Work on this data should be undertaken over the secure VPN connection using LVRPA provided equipment.

Users are required to ensure that they have up to date Antivirus/Malware software installed on their personally owned computers prior to any LVRPA work being undertaken on them.

Personal PC's are not permitted to be attached to the Authority's network under any circumstances and personal peripherals such as external hard drives, printers and scanners must be checked and approved by I.T before being connected to a Authority PC as relevant drivers will need to be provided by staff.

Users are advised that the I.T department does not support personal I.T equipment

12.2 Bring your own devices (BYOD)

In order to protect the confidentiality of sensitive data and the integrity of the Authority; e-mail accounts will not be set up on a user's personal device until an employee has worked for the Authority for at least 3 months or until their probationary period has been satisfactorily completed.

A line manager must approve in writing that e-mail can be set up on a user's personal device. Once approved, E-mail accounts must be set up by a member of the I.T department only.

A passcode must be set up and kept active on a user's personal device that has Authority's e-mail set up on it. Failure to keep this will result in the user's account being disabled until the e-mail account can be removed from the device. E-mail will not be set up on a user's personal device if the device does not have the ability to apply a passcode lock.

The Authority reserves the right to remotely wipe any user's device if the device is lost or stolen or if it is felt there is a risk to Authority.

The I.T manager reserves the right to refuse to set up e-mail on a user's personal device at any time if they feel the reasons for having it are not justified.

It is the user's responsibility to immediately report to I.T if their device is lost or stolen.

13. HARDWARE & SOFTWARE

I.T hardware and software must not be purchased and/or installed without the approval of the I.T Manager.

All I.T equipment must be asset tagged and its information recorded on the I.T asset register. Asset tags must not be removed from any I.T equipment. The I.T department must be contacted if an asset tag is missing or has been removed.

13.1 Security of Hardware

All items of hardware should be kept secure at all times. Hardware should not be left un-attended or left where it can be removed without authorisation. Users should take steps to secure hardware by using PC locks to secure PC's to desks, to reduce the risk of theft. PC locks will need to be purchased by the venue.

13.2 Loss or Damage to I.T. Equipment

If an item of I.T. equipment becomes damaged or is stolen it must be reported to the I.T. section immediately. Users must not attempt to repair or modify any equipment themselves.

All PCs and associated equipment (printers etc.) may only be repaired by an approved supplier, with the prior permission of the I.T. Manager.

13.3 Mis-use of Hardware

Hardware can be costly pieces of equipment and as such Staff should take steps to ensure that they are kept secure and are not damaged; this may include purchasing protective cases and not leaving the phone unattended at any time.

Mis-use of hardware will be construed as:

- Leaving hardware un-attended, which results in the device being lost or stolen
- Tampering with the hardware or software
- Allowing non-approved users to use the hardware
- Using the hardware for purposes other than what it is designed for
- Defacing or allowing the hardware to become defaced
- Fluid damage i.e. spilled drinks on hardware
- Persistent damage i.e. repeatedly persistently dropping the hardware etc.

If mis-use of hardware is identified the user will be charged the cost of the repair or replacement of the device.

13.4 Hardware Replacement

There is a rolling replacement scheme in place for the replacement of hardware. Once a piece of hardware has reached the end of its warranty/guarantee term it will either be replaced, refurbished or have the warranty/guarantee extended.

There is no automatic upgrade/replacement of hardware; however in some cases where for example the firmware / operating system is out of date and cannot be updated on the current hardware then an automatic replacement will apply.

13.5 Vendors

The I.T. section uses certain manufacturers when purchasing equipment, this is to ensure that they can be supported once purchased.
The current manufacturers used are:

- Dell and Microsoft for all PC's.
- Apple for iPhones and Nokia for standard mobile phones
- HP and Konica Minolta for all Printers and scanners.

I.T. section should be consulted if a piece of I.T. equipment is required that is not from one of these manufacturers.

13.6 Peripherals

If employees require replacement items of equipment such as laptop batteries, ink cartridges, toners, screens, keyboards etc. they should inform the I.T. section in writing what is required and supply a budget code for it to be purchased against.

13.7 Ink Cartridges

In most cases ink cartridges and toners can be purchased without going through the I.T. section. Only genuine HP ink cartridges and toners should be used.

13.8 Printers & Multi-Function devices (MFD)

The LVRPA provides MFD's for printing, scanning and copying. Local printers are supported but should no longer be purchased and will not be replaced if the printer becomes faulty.

Only genuine toners and cartridges should be used in printers. The cost of replacing these will be at the expense of the venue. The I.T department can advise on what toner or cartridges to order.

13.9 Disposal of Equipment

All I.T equipment (except for Keyboards and Mice) must be returned to the I.T department when it is no longer in use or needed. The I.T department will then arrange for the proper disposal, sale or re-assignment of the equipment in line with Authority guidelines.

14. INTRANET / PUBLIC FOLDERS

The Authority has its own internal website, which is known as 'Compass', where information can be stored and shared with all users of the Authority. Compass can be accessed via any internet browser and is also optimised to be viewed on mobile devices.

Compass is hosted externally and as such can be viewed by users when not on the network. Access to sections within Compass is controlled by security groups to prevent un-authorised access. If a user requires access to a section, their line manager must make the request in writing to itsupport@leevalleypark.org.uk.

Compass has replaced public folders, (which used to be accessed via Outlook) as Public Folders are no longer be available.

All users by default will have access to Compass, regardless of whether they are issued with LVRPA I.T equipment. If a user does not have exclusive access to LVRPA I.T equipment, their line manager must arrange suitable and convenient access to a shared LVRPA PC.

14.1 Acceptable Use

Compass is provided by the Authority and therefore the same rules apply with regards to acceptable use as defined in the 'Acceptable use of I.T' section in this policy.

MISCELLEANEOUS

14.2 Non-Compliance

Failure to comply with any of the provisions of this usage policy will result in disciplinary action in accordance with the normal procedures of the Authority, including, in extreme circumstances, termination of employment.

14.3 Incident Handling and Data Protection

The Authority will investigate complaints received from both internal and external sources, about any unacceptable use of email or I.T. The I.T department, in conjunction with other departments as appropriate, will be responsible for the collation of information from a technical perspective. It should be noted that logs are only kept for limited periods of time so the prompt reporting of any incidents which require investigation is recommended.

Where there is evidence of an offence it will be investigated in accordance with the Authority's disciplinary procedures applicable to all members of the Authority. In such cases The I.T department will act immediately with the priority being preventing any possible continuation of the incident. User accounts may be closed or email may be blocked to prevent further damage or similar incidents occurring.

14.4 Further Help and Guidance

If you have any queries about this policy or I.T. usage generally, please contact the I.T. Manager.

********** END OF DOCUMENT **********

Please now sign the IT Usage Policy declaration and return (only the signed declaration) to the I.T department.

I.T Usage Policy Declaration

Signing this form

The I.T. Usage Policy may alter from time to time and the updated I.T. Usage Policy will be available on Compass. Please review the I.T. Usage Policy regularly to ensure you are aware of any changes. Your continued use of I.T. equipment, services and systems after changes are posted means you agree to this I.T. Usage Policy as updated and/or amended.

I confirm that I have read, understood, accept and will abide by the requirements as set out in the I.T. Usage Policy.

I confirm that any personally owned equipment that I may use to carry out Lee Valley Regional Park Authority work has up to date Antivirus/Malware software installed, which I will ensure is regularly kept up to date.

User accounts will not be activated until this declaration has been received.

Print Name .....

Department/Venue.....

Signature.....Date.....

Please return the signed declaration to:
I.T Department,
Lee Valley Regional Park Authority,
Myddelton House,
Bulls Cross,
Enfield,
EN2 9HG