Confidentiality and Data Protection Policy

Contents

Confidentiality and Data Protection Policy

1. Aims and Objectives  
2. Principles  
3. Definitions  
4. Informed Consent  
5. Employee Responsibilities  
6. Compliance  
7. Cardwave’s Designated Data Controller  
8. Data Security  
9. Rights to Access Information  
10. Publication of Cardwave’s Information  
11. Retention of Data  

Management System

<table>
<thead>
<tr>
<th>Cardwave Policy:</th>
<th>Confidentiality &amp; Data Protection Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue: 1.1</td>
<td>Checked &amp; Issued by: Amy Johnson</td>
</tr>
<tr>
<td>Date: 16/07/2013</td>
<td>Authorised by: Anne Tew CFO</td>
</tr>
</tbody>
</table>
1. **Aims and Objectives**

1.1. This policy is set out to identify how Cardwave Services Ltd (Cardwave) executes its duty to keep personal information safe and confidential whilst at the same time, not compromising its ability to share information where it is needed.

1.2. The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within the organisation including volunteers and have access to personal information.

1.3. Cardwave is committed to maintaining the confidentiality of personal information that it handles. Any information given or received in confidence for one purpose will not be used for another purpose, or passed to a third party, without their consent except in special circumstances e.g. to prevent harm to an individual.

1.4. Cardwave will ensure that personal information is obtained, used and disclosed in accordance with the common law duty of confidentiality and the Data Protection Act 1998.

1.5. Cardwave will also have full regard for current and future legal requirements which impinge on the confidentiality of:

   1.5.1. Personal information in general, and
   
   1.5.2. Specific categories of personal information e.g. rehabilitation of offenders.

2. **Principles**

In accordance with the Principles of the Data Protection Act, personal information held in both computerised and manually filed records will:-

2.1. Be obtained and processed fairly and lawfully,

2.2. Be used only for the specified purposes for which it was obtained and not in any manner incompatible with those purposes,

2.3. Be adequate, relevant and not excessive for those purposes,

2.4. Be kept accurate and where necessary up to date,

2.5. Not be kept longer than is necessary for those purposes,

2.6. Be processed in accordance with individuals’ rights under the Act,

2.7. Be protected from unauthorised access, unlawful processing, accidental loss, destruction or damage,
Not be transferred to a country, which does not ensure adequate protection for the rights of individuals in relation to the processing of personal information. In order to implement and properly maintain a robust information security function, Cardwave recognises the importance of:

2.8. Understanding Cardwave’s information security requirements and the need to establish policy and objectives for information security;

2.9. Implementing and operating controls to manage Cardwave’s information security risks in the context of overall business risks;

2.10. Ensuring all users of Cardwave’s information assets are aware of their responsibilities in protecting those assets;

2.11. Monitoring and reviewing the performance and effectiveness of information security policies and controls; and

2.12. Continual improvement based on assessment, measurement, and changes that affect risk.

3. Definitions

3.1. ‘Confidentiality’ applies to information whether received through formal channels (e.g. in a formal report), informally, or discovered by accident. It applies to organisational business, employees and potential employees, volunteers, learners, clients, individuals, or organisations that come into contact with the organisation i.e. external contractors/partners.

3.2. Information which can be classified as ‘Confidential’, can broadly be grouped into the following areas:-

3.2.1. Information of a specific and personal nature about learner / clients, employees or volunteers

If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others.

3.2.2. Sensitive organisational information

This may be used to damage the organisation and other organisations, as well as individuals, staff or volunteers. It may be prejudicial to the business of the organisation or used to threaten the security of its property and systems.

3.3. Breaches in confidentiality happen when sensitive information is given to people who are not authorised to access it. They are most likely to happen when procedures have not been

3.4. Information security is the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, and reliability can also be involved, agreed or followed. They can also happen when information is passed between sections, or organisations, or when information is being stored insecurely.
4. **Informed Consent**

4.1. Where it is proposed, in exceptional circumstances, that information about an individual should be shared with another agency or person, the consent of the individual, or the person who provided the information, should normally be sought.

4.2. This should be done in such a way that those persons know exactly what information will be passed on, to whom and for what purpose.

4.3. Information, which is confidential and restricted, will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

4.4. Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information.

4.5. Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorised person.

4.6. Confidential information will not be discussed on the telephone unless the identity of the caller is established, this will be checked when necessary, e.g. with call-backs and/or security checks prior to the release of any information.

4.7. Refusal to give consent should be respected wherever possible.

5. **Employee Responsibilities**

5.1. In normal circumstances, staff may only disclose personal information outside the organisation if one or more of the following applies:

5.1.1. The disclosure is routinely necessary for the purpose for which the information is held and the individuals about whom the data is held have been made aware of, or could reasonably expect, such a disclosure to be made;

5.1.2. The disclosure is a legal requirement under the legislation governing the operation of the service or function concerned;

5.1.3. The receiving staff member ‘needs to know’ the information in order to carry out their duties;

5.1.4. The person about whom the information is held has given valid consent to the disclosure

5.2. Where it is not possible to obtain valid consent, information may exceptionally be passed on when there is a legal basis for overriding the usual non-disclosure e.g.
5.2.1. The disclosure is required under direction of a Court Order, or in the course of law enforcement, e.g. Trading Standards co-operation with other law enforcement agencies;

5.2.2. The disclosure is provided for agreed inter-agency procedures which have a legal basis for their operation, e.g., Sex Offenders Register, Mental Health Supervision Register, Public Protection Unit;

5.2.3. Where this is an overriding public interest in disclosing the information such as evidence of a risk of serious harm to the individual or in order to prevent or detect a serious crime.

5.3. When passing information to others, staff should:

5.3.1. Check that the source of the request is bona fide;

5.3.2. Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;

5.3.3. Only send the information necessary for the purpose of the disclosure;

5.3.4. Record exactly what has been passed on, to whom, when and why.

5.4. When receiving information from others, staff should:

5.4.1. Ensure that any information received in confidence should be marked as such to ensure it is not inadvertently disclosed to third parties;

5.4.2. Ensure that only information necessary for the purpose of the information being shared should be requested.

5.4.3. Ensure that information requests include a confidentiality statement similar to “Information will be treated with utmost confidence and will not be divulged to anyone outside the organisation except when stated at collection or agreed at a later date.” All confidential information shall be treated in line with Cardwave’s Confidentiality & Data Protection policy. A copy can be requested from the Company Secretary.

5.5. No reference to the company, its customers, suppliers or the work it undertakes must be made verbally or in any correspondence outside the company, in particular through social networking methods. Any information or reference to Cardwave passed through social networking must be approved in advance by the CEO.

5.6. Before sharing sensitive commercial information with suppliers or customers, a signed non-disclosure agreement (NDA) must be in place to ensure confidentiality is maintained.

All staff employment job descriptions and volunteer role descriptions must contain a statement enforcing the duty to respect the confidentiality of information. The employee handbook must include this obligation which then forms part of the employee’s contract / volunteer’s agreement.
5.7. Staff, students, staff of other agencies, temporary staff and volunteers will be asked to sign declarations of confidentiality on commencing employment with Cardwave either as part of their staff contract or as a separate statement.

5.8. All employees and volunteers are responsible for:

5.8.1. Checking that any personal data that they provide to Cardwave is accurate and up to date.

5.8.2. Informing Cardwave of any changes to information which they have provided, e.g. changes of address.

5.9. Sensitive information is only to be requested on a ‘need to know’ basis. This means only when the information is necessary to provide a service or to manage the delivery of a service effectively, and then only in the best interest of service users or staff.

6. **Compliance**

6.1. Cardwave will ensure that staff, volunteers and trustees receive adequate training and guidance on their duties and responsibilities in relation to the handling, disclosure and storage of personal information and information assets and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse.

6.2. Managers must ensure that staff and volunteers are made aware of the limits of their responsibilities, and where they may seek advice, should they have an information request which falls outside their responsibilities.

6.3. In accordance with the organisation’s disciplinary procedures, disciplinary action will be taken against any member of staff who fails to carry out the duties and responsibilities set out in this Policy or the procedures that follow from it.

6.4. Where contractors and employment agencies are used, the contracts between Cardwave and these third parties will contain clauses to ensure that contract staff are bound by the same code of confidentiality as employed staff.

6.5. Procedures will be implemented to ensure an employee’s, contractors or third party’s exit from Cardwave is managed and the return of all equipment and removal of all access rights are completed.

6.6. Any breach of this policy will be taken seriously and may result in formal action. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their line manager or the Company Secretary in the first instance.
7. **Cardwave’s Designated Data Controller**

Cardwave is responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Chief Executive. The Information Compliance Manager is the Company Secretary and any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Company Secretary.

8. **Data Security**

8.1. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

8.1.1. Any personal data which they hold is kept securely, either electronically or in lockable cabinets

8.1.2. Personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

8.1.3. Information taken off site must only be exceptional circumstances and must be recorded on an appropriate form (See appendix 2) and authorised by the CEO or Company Secretary. The staff member must ensure it is kept securely offsite at all times

8.2. Documents containing individual data must not be left visible where it can be read by anyone inappropriately. This includes telephone messages, computer prints, letters and other documents.

8.3. Desks must be cleared each evening and electronic documents closed down when leaving a desk. Office layout should take the responsibility for personal data into consideration.

8.4. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords.

8.6. All hardware containing data must be housed in a secure environment.

8.7. Personal data must not be stored on the hard disc of a laptop or flash drive unless it has been encrypted.

8.8. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner including sufficient firewall.

8.9. Protection will be required commensurate with the risks when using mobile computing and remote working facilities. See you protocols for controlling portable and removable storage devices (appendix 3)
8.10. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with Cardwave’s policies.

8.11. The physical and environmental security will prevent unauthorised physical access, damage, theft, compromise, and interference with Cardwave’s information and facilities. Locations housing critical or sensitive information or information assets will be secured with appropriate security barriers and entry controls. Secure areas will be protected by appropriate security entry controls to ensure that only authorised personnel are allowed access.

9. Rights to Access Information

9.1. Data is classified into different categories according to the sensitivity and usage (See appendix 4).

9.2. In accordance with individuals’ rights of access under the Data Protection Act, Cardwave will, on request, inform an individual whether or not information is kept about them and, if so, will provide a copy of that information. Any person who wishes to exercise this right should make the request in writing to the Company Secretary using the standard form. See Appendix I.

9.3. Cardwave reserves the right to charge the maximum fee payable currently £10 for each subject access request. If personal details are inaccurate, they can be amended upon request. The only exceptions to this are current employees who are not charged for access to records held in connection with their employment.

9.4. Cardwave aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 30 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

9.5. All individuals who are the subject of personal data held by Cardwave are entitled to:

9.5.1. Ask what information the organisation holds about them and why.

9.5.2. Ask how to gain access to it.

9.5.3. Be informed how to keep it up to date.

9.5.4. Be informed what the organisation is doing to comply with its obligations under the 1998 Data Protection Act.

10. Publication of Cardwave Information / Social Media

10.1. Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on customers contained within properly authorised externally
circulated publications. Any individual who has good reason for wishing details in such publications to remain confidential should contact the Company Secretary.

10.2. Under no condition should staff or contractors publish or discuss information about Cardwave through personal social media whether or not they consider the information to be confidential. Exceptions would need approval by the CEO.

11. **Collection and Retention of Data**

11.1. Any personal data collected that is not in the public domain should have the permission of the person relating to the information. Any business sensitive data should be agreed by a non-disclosure agreement (C-04). In all cases the purpose for holding such data should be clear. Data with no clear purpose should not be collected or retained.

11.2. Cardwave will keep some forms of information for longer than others depending on a number of factors e.g. customer requirements. All staff are responsible for ensuring that information is not kept for longer than necessary.

11.3. Disposal of information no longer required must be with regard to confidentiality, shredding paper documents and destroying other data in an appropriate manner.

11.4. The purpose for holding personal data and a general description of the categories of people and organisations to whom we may disclose it are listed in the Data Protection register. This information may be inspected or obtained from the Company Secretary.

11.5. The content of each filing cabinet and each archive box is recorded on the filing cabinet and archive box lists.

12. **Information Security Audit and Incident Management**

12.1. Auditing of the various processes around data management is built into the standard audit cycle to ensure compliance with this policy.

12.2. Information security incidents will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures will be established and communicated to all users. Responsibilities and procedures will be established to handle information security incidents once they have been reported.
SUBJECT ACCESS INFORMATION REQUEST FORM

Under the Data Protection Act 1998, you are entitled to request access to personal information held about you by Cardwave. Completing this form will help to locate your information quickly and efficiently.

Section 1 – Proof of identification

In the boxes below, give details of the name of the person completing this form:

Surname: ____________________________  Forename (s): ____________________________

Previous/alternative names: ___________________________________________________

Date of Birth: _______________________

Current address

House/flat no & Street: _____________________  Town/City: _________________________

County: _______________________________  Postcode: ____________________________

Telephone/mobile no: _____________________  Email: ____________________________

If you are the data subject or acting on behalf of the data subject please provide original proof of your identity bearing your name and address (i.e. passport, driving licence, birth certificate (or certified copy) or at least 2 official letters – e.g. from a utility company).

If you are acting on behalf of the data subject, please see section 2.

Please state below what evidence you have enclosed (please tick):

Birth Certificate □  Passport □  Driving Licence □  2 or more official letters □

Section 2 – Acting on behalf of data subject (if applicable)
If you are acting on behalf of the data subject with their written or other legal authority, please state your relationship with the data subject e.g. parent, legal guardian, or solicitor and the purpose for which the data is being collected (see notes attached)

Please enclose proof that you are legally authorised to obtain this information. The proof could be a letter of authority, letters or official forms addressed to you on behalf of the data subject. Photocopies cannot be accepted. Once entitlement has been established, we will take a copy of the documents you have supplied to us and will return the originals to you.

Please state below what proof of authority you have enclosed (please tick):

Letter of authority ☐  Correspondence ☐  Official Forms ☐

Section 3 – Data subjects details (before completion please see notes attached)

Data subject’s details (if different from Section 1):

In the boxes below, give details of the name of the person of the data subject request

Surname: ____________________________  Forename(s): ____________________________

Previous/alternative names: ___________________________________________________

Date of Birth: ____________________________

Current address:

House/flat no & Street: ____________________________  Town/City: ____________________________

County: ____________________________  Postcode: ____________________________

Telephone/mobile no: ____________________________  Email: ____________________________

Additional personal information
Please provide details of any additional information i.e. previous address you feel may be of assistance to this request:

___________________________________________________________________________________________

_________________________________________________________________________________________

Section 4 - Declaration

Please read the following declaration carefully, then sign and date it. Please note that any attempt to mislead may result in prosecution.

I, _______________________________ (name) certify that the information provided on this application to Cardwave is true. I understand that it is necessary for Cardwave to confirm my/the data subject’s identity and that it may be necessary for Cardwave to request more details from me in order to be able to locate the correct information.

Print Name: __________________________

Signature: __________________________ Date: __________________________

OFFICIAL USE ONLY:

Date received: _______________________ Identity confirmed: ___________________

Enquiry Log No: _______________________ Date responded: ___________________

NOTES:
Consent to application by a Third Party: Under the Data Protection Act 1998, an individual is entitled to ask Cardwave for a copy of personal information, which it holds, about him/her for the purposes of providing services to the individual. The information, which the individual is entitled to receive from Cardwave includes a description of these purposes, recipients to whom the data are disclosed and the sources of the data. This entitlement is known as the ‘Right of Access to Personal Data’. This access may also be granted by another person acting on behalf of the data subject providing written consent is given by the data subject.

Please note that in general requests for information about a person other than yourself will be rejected except in the following situations.

- Parents can request information about their children if they are under 16 years of age although there is not automatic right to the data.

- A solicitor may request information on behalf of a client
REQUEST TO REMOVE CONFIDENTIAL PAPERWORK / DATA FROM CARDWAVE PREMISES

<table>
<thead>
<tr>
<th>Description of paperwork / data e.g. supplier names, personal details, financial info etc.</th>
<th>Reason for removal from site</th>
<th>Date out</th>
<th>Date in</th>
<th>Requested by</th>
<th>Approved by Manager (If not a manager)</th>
<th>Approved by CEO / Company Secretary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mobile Device Security Protocols

Introduction

This policy describes the controls necessary to minimise information security risks affecting Cardwave’s laptops, mobile phones and other removable storage devices.

All Cardwave computer systems face information security risks. They are essential business tools but their very portability makes them particularly vulnerable to physical damage or theft. Furthermore, the fact that they are often used outside Cardwave’s premises increases the threats from people who do not work for the company and may not have its interests at heart.

Portable devices are especially vulnerable to physical damage or loss, and theft, either for resale (opportunistic thieves) or for the information they contain (industrial spies).

Do not forget that the impacts of such breaches include not just the replacement value of the hardware but also the value of any Cardwave data on them, or accessible through them. Information is a vital Cardwave asset. We depend very heavily on our computer systems to provide complete and accurate business information when and where we need it. The impacts of unauthorised access to or modification of, important and/or sensitive Cardwave data can far outweigh the cost of the equipment itself.

Physical security controls for mobile devices

The physical security of ‘your’ device is your personal responsibility so please take all reasonable precautions. Be sensible and stay alert to the risks.

- Keep your device in your possession and within sight whenever possible, just as if it were your wallet or handbag. Be extra careful in public places such as airports, railway stations or restaurants. It takes thieves just a fraction of a second to steal an unattended device.
- If you have to leave your laptop temporarily unattended in an office, meeting room or hotel room, even for a short while, use a laptop security cable or similar device to attach it firmly to a desk or similar heavy furniture. These locks are not very secure but usually deter casual thieves.
- Lock a device away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a device visibly unattended in a vehicle. If absolutely necessary, lock it out of sight in the trunk or glove box but it is generally much safer to take it with you.
• Carry and store a laptop in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. Don’t drop it or knock it about. An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.

• Keep a note of the make, model, serial number and the Cardwave asset label of your device but do not keep this information with the device. If it is lost or stolen, notify the Police immediately and inform your manager as soon as practicable (within hours not days, please).

**Virus protection of laptops**

• Viruses are a major threat to Cardwave and laptops are particularly vulnerable if their anti-virus software is not kept up-to-date. The anti-virus software MUST be updated daily. The easiest way of doing this is simply to log on and connect to the internet for the automatic update process to run. If you cannot log on for some reason, contact the IT Help Desk (IT 365) for advice on obtaining and installing anti-virus updates.

• Email attachments are now a major source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.

• Always virus-scan any files downloaded to your computer from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically but the IT Help Desk can tell you how to initiate manual scans if you wish to be certain.

• Report any security incidents (such as virus infections) promptly to the IT Help Desk in order to minimise the damage.

• Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting the IT Help Desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.

• Be especially careful to virus-scan files before you send any files outside of Cardwave. This includes EMAIL attachments and any physical media that you create.

**Controls against unauthorised access to data**

• You must use approved encryption software on all company devices, choose a long, strong encryption password/phrase, where possible and keep it secure. Contact the IT Help Desk for further information on encryption. If your device is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.

• You are **personally accountable** for all network and systems access under your user ID, so keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or IT staff.
Company laptops are provided for official use by authorized employees. Do not loan your laptop or allow it to be used by others such as family and friends.

Avoid leaving your laptop unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine.

Other controls for laptops

Unauthorized software
Do not download, install or use unauthorised software programs. Unauthorised software could introduce serious security vulnerabilities into the Cardwave network as well as affecting the working of your laptop. Software packages that permit the computer to be ‘remote controlled’ (e.g. PCanywhere) and ‘hacking tools’ (e.g. network sniffers and password crackers) are explicitly forbidden on Cardwave equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.

Unlicensed software
Be careful about software licences. Most software, unless it is specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and Cardwave into disrepute by breaking the law.

Backups
Unlike desktop PCs which are backed up automatically by IT, you must take your own backups of data on your laptop. The simplest way to do this is to logon and upload your data from the laptop to the network on a regular basis – ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks or hard drives, etc. Make sure that off-line backups are encrypted and physically secured. Remember, if the laptop is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the laptop. Off-line backups will save you a lot of heartache and extra work.

Laws, regulations and policies
You must comply with relevant laws, regulations and policies applying to the use of computers and information. Software licensing has already been mentioned and privacy laws are another example.
Security policies apply to all mobile devices, the data they contain, and network access (including use of the Internet).

**Inappropriate materials**
Cardwave will not tolerate inappropriate materials such as pornographic, racist, defamatory or harassing files, pictures, videos or email messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop and steer clear of dubious websites. IT staff routinely monitor the network and systems for such materials and will report serious/repeated offenders and any illegal materials directly to management, and disciplinary processes will be initiated. If you receive inappropriate material by email or other means, delete it immediately. If you accidentally browse to an offensive website, click ‘back’ or close the window straight away. If you routinely receive a lot of spam, call the IT Help Desk to check your spam settings.

**Health and safety aspects of using laptops**
Laptops normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Limit the amount of time you spend using your laptop. Wherever possible, place the laptop on a conventional desk or table and sit comfortably in an appropriate chair to use it. If you tend to use the laptop in an office most of the time, you are advised to use a ‘docking station’ with a full-sized keyboard, a normal mouse and a display permanently mounted at the correct height. Stop using the device and consult your Health and Safety representative for assistance if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the portable.

**Acceptable Use of Other Mobile Devices**
End Point data storage devices covers the storage of data on devices that can be connected either by a USB drive, data cable or by wireless connection direct to any computing equipment within the company; e.g.,

- USB sticks, drives, thumb nails, pen drives, flash drives, etc
- iPods
- Cameras with USB drive connection
- iPhones / Smartphones
- Bluetooth,
- WiFi
- PCI / PC Card / PCMCIA
- PDAs
- Other data storage devices (CDROM, DVD)
**USB data storage devices**

Cardwave supplies approved data storage devices for business purposes and sensible use is to be made in the ordinary course of business operations.

Personal use is not permitted of these USB data storage devices.

The connection of privately owned USB data storage devices to the organizations computers is not permitted.

**Responsibilities**

All end users of computing systems located within Cardwave are responsible for ensuring that they understand and comply with this acceptable use policy.

Proper use and protection of data, resources and information is essential for business performance and continuity of business operations.

Loss of data through end point data devices places the organization at risk of competitive advantage, competition, and viability so it is important that each end user understand and accepts responsibility for their own actions at the entry point where data is utilized on day to day business operations.

It is each end users responsibility and obligation to ensure that all end point data devices, where approved for use, are used only for its intended business purpose and that information contained or transmitted via these resources are protected from unauthorized use, copying or modification for personal advantage.

It is essential that you review read, understand, and agree to the terms of this policy.

Management has a responsibility to provide sensible use access to these devices to provide the most effective and efficient form of business operations, with the understanding by end users that with the use of these devices, the responsibility rests with the end user to protect the organizations data at all times.

Management will act responsibly in terms of monitoring usage of these devices and will alert end users when devices are being used in day to day operations so that each end user needs to understand that usage data is being logged as it occurs and will be periodically monitored to observe for violations of this policy.
<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
<th>SAMPLE DOCUMENTS / RECORDS</th>
<th>MARKING</th>
<th>PHYS &amp; ADMIN CONTROLS</th>
<th>REPRODUCTION</th>
<th>DISTRIBUTION</th>
<th>DESTRUCTION/ DISPOSAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUBLIC or open</td>
<td>Information that may be distributed without causing damage to the organisation, its employees and stakeholders. The Managing Director must pre-approve the use of this classification. These documents may be disclosed or passed to persons outside the organisation.</td>
<td>Marketing materials authorised for public release such as advertisements, brochures, published annual accounts, Internet Web pages, catalogues, external vacancy notices</td>
<td>None</td>
<td>None</td>
<td>Unlimited</td>
<td>No restrictions</td>
<td>Recycling/shredding</td>
</tr>
<tr>
<td>INTERNAL or proprietary</td>
<td>Information whose unauthorised disclosure, particularly outside the organisation, would be inappropriate and inconvenient.</td>
<td>Most corporate information falls into this category. Company memos, training materials, policies, operating procedures, work instructions, guidelines, phone and email directories, marketing or promotional information (prior to authorised release), Transaction data, productivity reports, disciplinary reports, contracts, Service Level Agreements, internal vacancy notices, Intranet Web pages</td>
<td>&quot;INTERNAL USE ONLY&quot; Apply to bottom left corner of each page.</td>
<td>Author: responsible for proper markings. User: responsible for proper storage and document control.</td>
<td>Limited copies may be made only by employees, or by contractors and third parties who have signed an appropriate nondisclosure agreement.</td>
<td>Internal: use and store on appropriate restricted network access, distribution to approved users by email if necessary. External: use a sealed envelope. Electronic: use approved email system. Encryption is required for transmission to external email addresses. FAXing: double check the FAX number!</td>
<td>Paper documents: shred. Electronic data: erase or degauss magnetic media. Pass all CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate erasure / disposal</td>
</tr>
<tr>
<td>CONFIDENTIAL or restricted</td>
<td>Highly sensitive or valuable information, both proprietary and personal. Must not be disclosed outside of the organisation without the explicit permission of the Managing Director.</td>
<td>Passwords and PIN codes, VPN tokens, credit and debit card numbers, personal information (such as employee HR records, National Insurance Numbers), most accounting data, other highly sensitive or valuable proprietary information</td>
<td>&quot;CONFIDENTIAL&quot; Apply to bottom left corner of each page.</td>
<td>Originator: responsible for ensuring that confidential information is distributed on a strict need-to-know basis. Recipient: responsible for ensuring that confidential information is encrypted and/or kept under lock &amp; key when not in use.</td>
<td>Limited copies may be made only by permission of originator or his/her designates. A signed authorisation will be recorded.</td>
<td>Internal: use a sealed envelope. Hand deliver if possible. External: use a plain sealed envelope. Hand deliver or send by registered mail, courier etc. Electronic: use approved email system only. Encrypt the data. FAXing: requires phone confirmation of receipt of a test page immediately prior to sending the FAX, and phone confirmation of full receipt.</td>
<td>Paper documents: shred using an approved cross-cut shredder. Electronic data: erase or degauss magnetic media. Pass CDs, DVDs, dead hard drives, laptops etc. to IT for appropriate erasure / disposal</td>
</tr>
</tbody>
</table>