Information Security at Advance

Policy and guidelines

Introduction

This document contains the Information Security Policy and associated guidelines of Advance Housing & Support Ltd ('Advance'). It is the property of Advance and is a controlled document. The purpose of the document is to explain Advance's policies about accessing, maintaining, managing and storing organisational data in a secure and controlled way.

Scope

The Information Security Policy covers all areas of Advance's activities in relation to maintaining the security of its proprietary information and data. This includes data stored on computers, memory sticks, transmitted across networks, printed out or written on paper, sent by fax, stored on disk or spoken in conversation or over the telephone.

Objective

Advance has created the Information Security Policy to ensure a consistent and controlled approach to the security of its proprietary information and data that supports compliance with all related contractual, legal and regulatory obligations, and in particular with reference to the General Data Protection Regulation (GDPR), and the standards set out in ISO27001 and the Advance Information Security Management System (ISMS).

Relevance

The Information Security Policy applies to Advance staff, Advance Board members, Advance volunteers, and organisations contracted to carry out duties on behalf of Advance.

Key Changes (Summary): The policy has been updated to support compliance with the General Data Protection Regulation (GDPR), to reflect changes to related policies and procedures, and the introduction of an email encryption and secure file transfer solution.

Related Policies:	Data Protection Policy Incident and Accident Reporting Policy Data Sharing Policy Social Media Policy Theft, Loss, Anti-Fraud, Anti-Bribery and Tax Evasion Policy Mobile Device Policy & Acceptable Use Guidelines CCTV Policy Customer Records Policy
Related Documents:	Advance Information Security Management System (ISMS) Code of Conduct

Administrative purposes only:

Policy owner:	Head of ICT & Business Systems	
Date written:	2013	**Version:** V1
Review written/refreshed by:	Head of ICT & Business Systems	**Date:** May 2018
Draft consulted upon with:	GDPR Project Team and The Voice (May 2018)	
Approved by: GMT	**Version:** V3.7	**Date of Approval:** 21 June

Why do we need an Information Security Policy?

As a provider of services to vulnerable adults, Advance is required to access, maintain, store and transmit confidential and sensitive information. This may take many forms including data stored on computers, memory sticks, transmitted across networks, printed out or written on paper, sent by fax, stored on disk or spoken in conversation or over the telephone.

We store, access and manage much of our confidential or sensitive information on computers and in software solutions. Therefore, it is important that we have a policy in place to:

- Protect the substantial investment in ICT and business systems;
- Safeguard the information in the systems;
- Reduce business and legal risk;
- Protect the good name of Advance;
- Uphold the rights of people who get services from us.

We also work with sensitive information in other forms including paper-based systems and verbal / written communications. It is important that we have a policy in place to ensure a commensurate standard of security when working with information in these media.

As employees, we have to take the security of our business information seriously, because:

- Computer systems are vulnerable to security threats, fraud, hacking or viruses;
- We have to comply with the laws relating to the handling of sensitive, confidential and personal information e.g. General Data Protection Regulation (GDPR);
- We are dealing with information relating to the lives of vulnerable people;
- Staff and other parties acting on our behalf need to know our expectations about security and physical or verbal data and information;
- Staff need to know what they may or may not do with the ICT equipment provided by Advance.

For all these reasons, we have a policy setting out the rules, expectations and individual responsibilities of staff in relation to security of information at work. And we ask staff to sign a declaration that they have read the policy and understand it.

Monitoring

Under the terms of General Data Protection Regulation (GDPR), we are entitled to monitor the content of work-related e-mail and Internet usage.

Any message created, sent, or retrieved using Advance equipment belongs to Advance and may be regarded as public information. So we may log and access the contents of any material communicated over our networks if we think that we have a business need to do so. We may also audit email and Internet use if we feel this is justified (like suspected copyright infringement or harassment), as long as employees know in advance that this is our policy.

Monitoring the content of personal e-mail / Internet use is a more involved issue. We will not examine the content of e-mails unless we suspect our system is being abused, and we may not do this without employees' consent. This is why we include an acknowledgement form, signing of which is deemed as giving this consent.

We comply with UK law, and will deal with any illegal use of our ICT equipment appropriately. In cases involving suspected illegal activity we may disclose relevant communications to the appropriate authorities without prior reference to or consent of the sender or the receiver.

Reporting a breach

Staff, the Board and customers are responsible for reporting possible or suspected personal data breaches (see Definitions Section in the Data Protection Policy).

Step 1: If you suspect that a personal data breach could have taken place:

(i) Immediately report this to your line manager or any other member of management at Advance (call the main Advance telephone number 0333 012 4307 and customer services or the out of hours service will help you).
(ii) Within 48 hours, you should log a serious incident report through the steps outlined on the Incident Reporting page of the intranet, following the guidance set out in the Incident and Accident Reporting Policy.

Step 2: Any manager receiving such a report must immediately inform all of the below:

- Director or Resources (who is the Data Protection Officer), AND
- The Head of ICT and Business Systems, AND
- The Head of Business Assurance.

The Director of Resources, the Head of ICT and Business Systems and the Head of Business Assurance will:

(i) Determine whether a breach has taken place.
(ii) If there has been a breach, an assessment will be made to decide if it is a notifiable breach i.e.is there a risk to individuals' rights and freedoms (referencing the guidelines set out on the ICO's website).
(iii) If it is a notifiable breach, then it must be reported to the ICO **within 72 hours of becoming aware of the breach.**
(iv) Inform the Chief Executive, Board members and GMT as appropriate.
(v) If relevant, inform the data controller where Advance is the data processor.
(vi) If there is a 'high risk' to individuals' right and freedoms then inform the individuals without undue delay.
(vii) Record all decisions and justifications and complete the Incident Report.

Discipline and other consequences

Any member of staff who violates this policy will be subject to appropriate disciplinary action or other remedial measures, up to and including termination of employment if warranted under the circumstances and permissible under applicable law.

What you must do

- Read the full policy before you use Advance ICT equipment or access any Advance information assets. If there is anything you don't understand, discuss it with your line manager.
- You must read and sign both copies of Appendix A, the 'Employee Acknowledgement of Information Security at Advance'. Send the second copy of the form to the HR department at Witney; keep the first copy with the policy.

1. Advance Data

Definition

We hold a lot of confidential and sensitive business information both electronically and in paper files. This includes:

- Financial information;
- New business ideas;
- Marketing strategies and plans;
- Databases and data;
- Customer records;
- Technical information;
- Computer software codes and computer/network access codes.

Policy

- You must avoid taking any action that knowingly threatens the normal operation of the Advance network, like propagating a virus or causing 'high volume' network traffic (for example, by emailing a very large file as an attachment to a lot of people).

- You may not look at or change other people's electronic or paper-based files without their authority.

- You must take care not to reveal confidential and sensitive business information in either paper-based or electronic format to people outside the organisation unless it is in our business interests to do so (for example, in tender submissions), and you must apply appropriate levels of security to any such transfer.

- Any data losses must be reported by following the procedure detailed earlier in this policy, and in line with the Theft, Loss, Anti-Fraud, Anti-Bribery and Tax Evasion Policy and the Incident Reporting Policy,

2. Ownership of Assets

Definition

Our information assets take many forms: they include data stored on computers, memory sticks, transmitted across networks, printed out or written on paper, sent by fax, stored on disk or spoken in conversation or over the telephone etc. We have controls in place to maintain the appropriate level of protection of information assets and equipment.

Policy

- You must sign this Information Security Policy before the organisation's information assets are released to you.
- Once you have been assigned information assets you are responsible for them. You must ensure that the assets are only used in accordance with company policy.

3. Data Transfer Devices

Definition

Data transfer devices include:

- Memory sticks;
- USB devices;
- CDS;
- DVDs;
- Digital video and still images.

Policy

You must use these for business reasons only. It is your responsibility to lock documents stored on these devices with a password, or encrypt them using the device software. All USB memory devices must be supplied by ICT, which will be password protected and will encrypt data.

- If you wish to use a USB stick, you will need to request one from ICT.
- Where possible you should avoid use of data transfer devices and make use of encrypted emails using Egress or the corporate Dropbox account. Information about both of these options is available from the ICT Service Desk.

Digital cameras and video

We welcome the use of digital cameras and camcorders as an aid to communication. Customers have the right to know that they are being photographed or filmed, why the photograph/video footage is being taken and by whom, so please bear in mind the following:

- Always get the consent of the person you are photographing or filming. Advance has consent forms to help with this, which are available from the Customer Engagement page of the intranet.
- Photography or video footage of service users taken at any kind of event organised by or associated with Advance is permitted for work use only, and can only be taken by people authorised to do so by an appropriate member of staff.
- Make sure you can transfer the data from the camera to your computer. If in doubt please log a call with the ICT Service Desk.
- Please refer to the CCTV policy for guidance relating to the installation, management and maintenance of CCTV equipment.

4. Computer Viruses

Definition

Computer viruses are designed to make unauthorised changes to programs and data. If our computer networks and systems became infected with a virus, the consequences could be very harmful to us. To prevent this happening we use antivirus software, but staff have a responsibility to minimise the likelihood of a virus being introduced into our network.

Policy

- Use only trusted sources for data and programs.
- Don't knowingly introduce a virus into Advance computers.
- Don't use unauthorised data transfer devices (CDs, DVDs, memory sticks or USB devices) if you can't identify or don't trust where they come from.
- Data transfer devices from an external supplier or source must be scanned for viruses, before you use the data. Please refer to the ICT Service Desk for instructions.
- If you think your workstation has been infected with a virus you must **turn the power off immediately** and log a call with the ICT Service Desk.

5. Access Control

Definition

By 'Access control' we mean those controls we have put in place to safeguard our electronic and physical information.

Passwords and electronic access control

We put user controls (such as passwords) in place to prevent unauthorized user access, compromise or theft of information and information processing facilities.

- You are responsible for all computer transactions that are made with your User ID and password. This includes database systems (like OPENHousing) and applications (like Adobe, or MS Word).
- Keep your login details safe, memorise them, and don't share them with anyone else.
- If you suspect someone knows your password then change it immediately, and report the incident to the ICT Service Desk.
- In any case, our systems will prompt you to change your password regularly. If you do not do this your password will expire and your account will be locked.
- Your password must be at least eight characters long, and contain at least one Capital letter and one number. Guidelines for secure password creation are available in the for the ICT & Business Systems page of the intranet.
- You must make your workstation secure when you leave it unattended for any length of time. To do this, press 'Ctrl', 'Alt' and 'Delete' simultaneously on your keyboard and select 'Lock Computer' from the menu that appears.
- You must not attempt to gain unauthorised access to operating systems and applications.

Physical access control

We put physical access controls in place to prevent unauthorized access to paper-based information held in physical locations or printed out from electronic sources.

- Filing cabinets – if you have a lockable filing cabinet, lock it. The keys should be kept in a secure location away from the cabinet. Do not leave keys in the lock.
- Clear desks – do not leave sensitive or confidential data lying around your desk. If you are moving away from your desk, clear it.
- Waste paper – all confidential data must be shredded and disposed of as appropriate.
- Paper-based data – if you are photocopying or scanning sensitive data, do not leave it in the copier or copier tray. Take responsibility for ensuring you remove it a soon as possible.
- All personnel that are directly involved with the control of records must ensure they follow the instructions shown in the relevant policy & procedures.

Asset classification

We need to ensure that all the information we receive, transmit, manage or store receives a classification, to help establish an appropriate level of protection. We classify all our information assets, whether electronic or paper-based, in line with the requirements of current data protection legislation and to meet the requirements of individual contracts.

- You must ensure that all information assets are correctly classified in line with requirements of the General Data Protection Regulation (GDPR) and any other contractual or regulatory requirements.
- You must ensure that all paper-based records are suitably classified and clearly marked with the appropriate level of classification.

Guidance on asset classification and protective marking is available in the Data Sharing Policy.

6. The Internet and Email

Policy

- The Advance email system is a business communication tool, so staff need to treat all emails like any other official Advance document. Customers and colleagues could have the legal right under the General Data Protection Regulation (GDPR) to see such documents.
- Emails should never contain unsubstantiated allegations or use anything other than businesslike and professional language.
- Advance will take disciplinary action against any member of staff who deliberately visits, views, downloads or publishes anything containing illegal, pornographic, racist, sexist or offensive material, or publishes indecent remarks, proposals or material via email or the Internet.

All emails are scanned daily for viruses and spam-like qualities. A standard company disclaimer is added to any emails sent externally. Any emails identified by our systems as viruses or spam are quarantined and periodically deleted.

Your responsibilities on Internet and email

- All communications must be solely for business reasons, other than during the 'personal use' time detailed below.
- You are responsible for the content of all text, audio, or images placed or sent by you via the Internet.
- You must attach your name to all communications sent, using the standard email signature.
- You must not transmit copyrighted materials without permission.
- You must abide by all applicable Advance policies dealing with security and confidentiality of its records.
- You must not send emails or attachments externally that contain confidential personal information without using the Egress email encryption and secure file transfer solution to secure the data during transfer.
- You must ensure that the antivirus software is functioning correctly.
- You must avoid transmission of private or sensitive service user information if at all possible. If this is unavoidable, you must make sure that you are sending the information to someone who is authorized to receive it for a legitimate use that is in the service user's best interests.
- If you are using the Internet or email to exchange information or communicate with people outside Advance you are representing Advance, so you must behave appropriately.
- Examples of acceptable business use include: using web browsers to obtain business information; accessing databases on commercial websites for information; using email for business communication; and broadcast purposes.

Guidelines for personal use – internet

- You may browse the Internet on Advance equipment for your own use before or after your working day or during your lunch break, on the understanding that you don't breach the guidelines in this policy.
- Acceptable personal browsing includes shopping, online banking, checking news, organising holidays.
- Access to social media is permitted for business use at any time and for personal use before or after your working day, during your lunch break, or on any other agreed break, on the understanding that you don't breach the guidelines in this policy. See the section on social media in this document for further information.

Guidelines for personal use – email

Advance's email system is meant for business use; personal use of the email system can only be permitted in occasional, exceptional or urgent situations (for example to let family know that you are delayed in returning home). The following guidelines must be adhered to:

- Personal use of email must not interfere with work and the individual's job responsibilities.
- It must also not affect the job responsibilities of other employees, disrupt the email system or harm the organisation's reputation.
- Non-work emails must adhere to the guidelines in this policy

Downloads

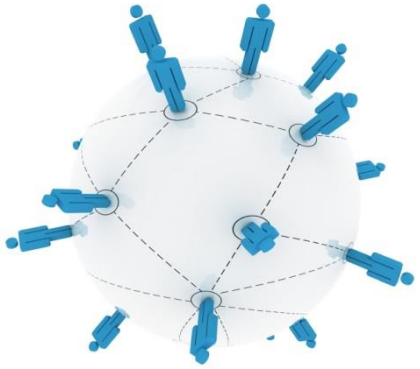
You may:

- download Word documents, PDF files, excel spreadsheets, and copy web pages – as long as there are no copyright limitations.

You may not:

- download files for installing on your PC (for example, '.exe' files) without authority from the ICT Service Desk.

7. Social Media



Definition
For the purpose of this document social media is defined as *any website, application (app) or medium that allows for open and shared online communication*.

Policy
The separately published Social Media Policy provides guidance for employee use of social media, which should be broadly understood for purpose of this policy to include blogs, wikis, microblogs, message boards, chat rooms, electronic newsletter, online forum, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner.

Principles
Advance recognises that social media can benefit social care in a variety of ways, including fostering professional connections, promoting timely communication and educating and informing consumers and health care professionals.

People we support have the right to access new and emerging technologies and staff have a role in supporting people to stay safe online. Staff should understand that such technologies offer huge opportunities to people, but also that online activity brings with it potential risks including accessing inappropriate content, predation and grooming, radicalisation, bullying and threats, identity theft, financial harm and corruption or misuse of data.

We also understand that social media tools such as blogs, micro-blogs, online forums, content-sharing websites and other digital channels established for online interaction and connection are increasingly used to share personal opinions and participate in online dialogue as individuals.

Employees are encouraged to make their friends, family members, professional networks and everyday contacts, aware of the activities of Advance, in a positive fashion, including, as appropriate, its presence in social media.

For further information and guidance please refer to the full Social Media Policy and the Code of Conduct available from the Policies and Procedures page of the Intranet.

8. Physical and Environmental Security

Our premises, ICT hardware and software are all valuable, and we follow certain controls to ensure their security in compliance with the standards set out in ISO27001, and as documented in the Information Security Management System (ISMS).

Physical security

We adopt controls around physical security to prevent unauthorised physical access, damage and interference to our premises and information.

- Advance uses physical security perimeters to protect areas that contain information and information processing facilities. The appointed person for each site holds the specification for these. You may not pass on any details about physical perimeters (for example, door access codes) to third parties.
- Advance uses physical entry controls to ensure that only authorized personnel are allowed access to secure areas. All staff are required to co-operate with requests relating to physical entry controls (for example wearing visitor passes/badges and keeping them visible, displaying ID cards). An appointed person for each site is responsible for maintaining physical entry controls.
- In a situation where you have arranged for third parties to gain temporary access via delivery or loading areas (for example a goods delivery, or a maintenance visit) you are responsible for supervising their attendance on site at all times.

Equipment security

We adopt controls around equipment security to prevent loss, damage, theft or compromise of assets and interruption to our activities.

- Store laptops and data transfer devices out of sight. Keep them locked up if they contain sensitive or confidential information.
- You must take care to keep safe the equipment that is assigned to you. If you don't, you may be liable. For example, you must never leave ICT equipment unattended in a car. The equipment would not be insured and you would be fully liable for any loss.
- Keep data transfer devices away from environmental hazards such as heat, direct sunlight and magnetic fields.
- Keep hardware away from food and liquids, high/low humidity and extreme heat/cold.
- Don't try to install, disconnect, modify or relocate ICT equipment. This is the ICT team's responsibility;

Mobile computing and teleworking

The same standards and expectations apply for mobile devices (including laptops, i-Pads, netbooks and smartphones) as for fixed workstations, to ensure information security when using mobile computing and teleworking facilities.

- You must make sure you make your mobile device secure if you leave it unattended.
- You must ensure, as far as is physically possible, to keep your work, files, emails or messages screened so that it cannot be easily seen by casual observers.

9. Copyright and Licence Agreements

We comply with all laws relating to copyright and licences – this applies to Advance and all employees, and to software that is owned by us, licensed to us, or developed by us or on our behalf.

The rules are simple:

- Don't install any software unless authorised by the ICT team;
- Don't copy any software unless authorised by the ICT team;
- Don't download any software unless authorised by the ICT team.

In addition:

- you may not transmit or share copyrighted commercial software or other copyrighted materials belonging to Advance or anyone else, without authority from the Head of ICT and Business Systems;
- You may not copy, transfer, rename, add or delete information or programs belonging to others without express permission from the owner – to do so may be a breach of copyright or licensing laws and could result in legal action by the owner and disciplinary action by Advance.

By breaching copyright or licence agreements you may leave yourself and Advance open to civil/criminal penalties.

Appendix: Employee acknowledgement of 'Information Security at Advance'

Employee copy

We use this form to acknowledge that you have read our policy on Information Security, and will comply with it.

What you need to do

1. Read the policy;
2. Sign and date both copies of this form;
3. Keep this page with the policy. Return the next page only to the HR department.

Signature

By signing this form, I agree to the following terms:

- I have received and read 'Information Security at Advance', and understand it and the associated policies;
- I will abide by the policy statements and instructions contained in each section of the policy;
- Any ICT equipment provided to me by Advance may contain confidential information about Advance and its clients, and remains the property of Advance at all times;
- I shall not copy, duplicate (except to make backup versions), disclose, or let anyone else copy or duplicate any of this information or software;
- If I leave Advance for any reason I will return all computer software and hardware provided by Advance during or prior to my employment;
- I understand that Advance may monitor my use of email and the Internet, and that they may inspect the content of communications sent and received and web pages visited.

Signature: .....

Name: .....

Date: .....

Directorate / Department: .....

Appendix: Employee acknowledgement of 'Information Security at Advance'

Copy to HR

We use this form to acknowledge that you have read our policy on Information Security, and will comply with it.

What you need to do

1. Read the policy;
2. Sign and date both copies of this form;
3. Return this page only to the HR department.

Signature

By signing this form, I agree to the following terms:

- I have received and read 'Information Security at Advance', and understand it and the associated policies;
- I will abide by the policy statements and instructions contained in each section of the policy;
- Any ICT equipment provided to me by Advance may contain confidential information about Advance and its clients, and remains the property of Advance at all times;
- I shall not copy, duplicate (except to make backup versions), disclose, or let anyone else copy or duplicate any of this information or software;
- If I leave Advance for any reason I will return all computer software and hardware provided by Advance during or prior to my employment;
- I understand that Advance may monitor my use of email and the Internet, and that they may inspect the content of communications sent and received and web pages visited.

Signature: .....

Name: .....

Date: .....

Directorate / Department: .....