GDPR

POLICY AND PROCEDURE

Date Policy Implemented August 2018 by Paul Graham – Director of Care
Policy Reviewed January 2023 by Rebecca Gritton- HR Manager

ASPECTS CARE
GDPR POLICY

Data Protection

Introduction

The EU General Data Protection Regulation ("GDPR") replaces the 1995 EU Data Protection Directive. The GDPR strengthens the rights that individuals have regarding personal data relating to them and seeks to harmonize data protection laws across Europe, regardless of where that data is processed.

Aspects Care Ltd is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with our legal obligations.

We hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes.

This policy sets out how we collect and process personal data and seek to protect personal data.

Data Controller and Contact Information

Aspects Care has appointed Paul Graham, Director of Services as the person with responsibility for data protection officer within Aspects Care. He can be contacted at paulgraham@aspectscare.co.uk. Questions about this policy, or requests for further information, should be directed to him.

Third-Party Links

Our website may include links to third-party website, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data. We do not control these third-party websites and are not responsible for their privacy statements.

Reasons/Purposes for Processing Information

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, process, store and transfer personal information to enable us to provide our care services; to maintain our own accounts and records; to support and manage our employees. We may also collect, process, store and transfer personal information by way of our CCTV systems to monitor and collect visual images for security and the prevention and detection of crime or by using audio recording equipment to record telephone calls for record or training purposes.

We may collect and process information relevant to the above reasons/purposes. This information may include:

- personal details including names, addresses, telephone numbers, email addresses, dates of birth, NHS numbers, National Insurance numbers.
- lifestyle and social circumstances
- financial details (including bank account details, payment card details and details about payments made to and from us to other people)
- education and employment details
- visual images of individuals, details regarding individual's personal appearance and behaviour
- technical information including internet protocol (IP) addresses, browser type and version, time zone setting and location, operating system and platform and other technology on devices used to access this website

We may also process special categories of personal data including:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- offences including alleged offences
- criminal proceedings, outcomes and sentences

We also collect, use and share aggregated data such as statistical aggregated data which could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate certain types of personal data to calculate the percentage of individuals who have a certain preference. However, if we combine or connect aggregated data with your personal data so that it can directly or indirectly identify you, we will treat the combined data as personal data, which will be used in accordance with this privacy policy.

Who the information is processed about

We process personal information about:

- service users
- personal representatives of the above
- complainants
- enquirers
- individuals captured by CCTV images
- offenders and suspected offenders
- employees and their next of kin

Who information is obtained from

The information we hold is obtained from:

- The subjects themselves
- Their next of kin or personal representatives
- Professional bodies engaged to represent the person
- Other data controllers for whom we are processing data (eg. Local Authorities)
- Government agencies providing data relevant to our business (together the "Sources").

How the information is obtained

We may use different methods to collect data regarding data subjects, including:

- Direct interactions. This is when personal data regarding a subject is obtained directly by any of the Sources by filling in hard copy forms or forms on our website or by corresponding with us by post, phone, email or otherwise.

- Automated technologies or interactions. As individuals interact with our website, we will automatically collect technical data about their equipment, browsing actions and patterns. We collect this personal data by using cookies and other similar technologies.

How we use your personal information

We will only use your personal data in the following circumstances:

- Where we need to perform the contract, we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal obligation.

Generally, we do not rely on consent as a legal basis for processing your personal data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us.

Change of purpose

We only use personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use personal data for an unrelated purpose, we will notify the data subject and explain the legal basis which allows us to do so.

Please note that we may process personal data without knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Who the information may be shared with

We sometimes need to share the personal information we process with the data subject and also with other organisations for the purposes of performing the contract we are about to enter into or have entered into, where it is necessary for our legitimate interests (or those of a third party) and the data subject's interests and fundamental rights do not override those interests or where we need to comply with a legal obligation. The types of organisations we may need to share some of the personal information we process with for the purposes set out above may include:

- healthcare professionals, social and welfare organisations with whom or for whom we carry out legitimate business
- The Care Quality Commission or other legitimate regulators of our business
- family, associates and representatives of the person whose personal data we are processing
- central and local government
- suppliers and service providers
- employment and recruitment organisations
- credit reference agencies
- debt collection and tracing agencies
- business associates and other professional advisers
- financial organisations
- current, past or prospective employers
- educators and examining bodies
- people making an enquiry or complaint
- police forces and security organisations
- data processors with whom we contract (eg. Payroll service providers)

Data Protection Principles

Aspects Care processes personal data in accordance with the following data protection principles:

- Aspects Care processes personal data lawfully, fairly and in a transparent manner.

- Aspects Care collects personal data only for specified, explicit and legitimate purposes.

- Aspects Care processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.

- Aspects Care keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.

- Aspects Care keeps personal data only for the period necessary for processing.

- Aspects Care adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

- Aspects Care tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data.

Where Aspects Care processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data.

Aspects Care will update personal data promptly if an individual advises that their information has changed or is inaccurate.

Rights of access, correction, erasure, and restriction

Under certain circumstances, by law you have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- Request the erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to stop processing personal data where we are relying on a legitimate interest and there is something about your particular situation which makes you want to object to processing on this ground.

- Request the restriction of processing of your personal data. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- Request the transfer of your personal data to another party.

- If you want to review, verify, correct or request erasure of your personal data object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact Human Resources.

Individual Responsibilities

Individuals are responsible for helping Aspects Care keep their personal data up to date. Individuals should let Aspects Care know if data provided to Aspects Care changes, for example if you move to a new house or changes your bank details.

You may have access to the personal data of employees, workers, contractors, customers, clients, suppliers or agents in the course of your employment. Where this is the case, Aspects Care relies on you to help meet our data protection obligations to these individuals.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;

- to keep data secure (for example by complying with rules on disclosure of data, access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices containing or that can be used to access personal data, from Aspects Care's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and not to store personal data on local drives or on personal devices that are used for work purposes.

Unauthorised use, processing or disclosure of personal data (including special categories of personal data), or any serious or deliberate breach of data protection policies or procedures may constitute gross misconduct and could lead to dismissal without notice.

<u>International Transfers</u>

We do not transfer any personal data outside of the European Economic Area.

Disclosure & Rights of Individuals

Individuals have rights to their data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be informed

Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.

Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

2. Right of access

Enabling individuals to access their personal data and supplementary information

Allowing individuals to be aware of and verify the lawfulness of the processing activities

3. Right to rectification

We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

4. Right to erasure

We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to restrict processing

We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.

We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

6. Right to data portability

We must provide individuals with their data so that they can reuse it for their own purposes or across different services.

We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

7. Right to object

We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.

We must respect the right of an individual to object to direct marketing, including profiling.

We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

8. Rights in relation to automated decision making and profiling

We must respect the rights of individuals in relation to automated decision making and profiling.

Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

Data Retention

We will only retain personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of the personal data, the purposes for which we process the personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

Staff Training

All staff working for Aspects Care must complete a full recruitment, selection and induction procedure and this includes specific training around GDPR issues and requirements. The information is detailed within the Staff Recruitment, Selection and Induction Policy.

All staff must complete statutory and mandatory training courses and the courses delivered includes:

- GDPR Stage One
- Accessible Information
- Information Governance
- Lone Working
- Recording Information

Manager and more senior staff will complete GDPR Stage Two training.

A Training Matrix is maintained by the HR Team and this details all the courses completed by staff, how long they are valid for and refresher training dates.

Staff Contract of Employment

Within the Staff Employment Contract there is a specific section relating to confidentiality of information and the requirements of staff to comply with it.

Aspects Care employs Kingfisher Employment Law Services to review and monitor its contracts of employment. Part of that service is to ensure contracts of employment contain a relevant confidentiality of information clause.

Disclosure and Barring Service (DBS) Checks

As part of the recruitment process all support staff must complete an Enhanced DBS disclosures check.

A copy of the details of the disclosure reference number is retained by the HR Team at Aspects Care Head Offices and the disclosure itself is retained by the staff member.

The Aspects Care DBS Policy details exactly how DBS's are completed and processed and managed by Aspects Care.

CCTV Systems

Aspects Care does not currently run or operate any CCTV systems within its services and as such has no liabilities under GDPR relating to CCTV systems. However, Aspects Care would operate any CCTV systems in accordance with its GDPR Policy and would comply with all relevant statutory guidelines and applicable legislation.

Should any CCTV system be installed it will be done with due reference to the ICO implementation recommendations - *In the Picture: a data protection code of practice for surveillance cameras and personal information". If a CCTV system is ever brought online, then an ICO notification will be submitted, and a CCTV Privacy Impact Assessment completed.

IT & Data Security

We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal data to those employees, agents, contractors and other third parties who need to be able to access the personal data to work effectively. They will only process personal data on our instructions and are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify any applicable regulator (ICO) of a breach where we are legally required to do so.

Transmitting Personal Information

Email, Post and Fax Other Methods

There are always risks associated with transferring personal information. Appropriate security must be used for every transfer in order to minimise risk. The severity and type of these risks will vary depending on the method of transfer. Examples of such risks include:

- Information being lost, damaged or intercepted in transit e.g. stolen laptops, lost memory sticks, opened envelopes
- Delivery service delivering mail incorrectly.
- Information being sent to the wrong address via e-mail, post or fax.
- Information received by the organisation but not delivered to the correct person.
- Personal information not being disposed of appropriately.
- Information that is deliberately transferred with criminal/fraudulent intent e.g. ID theft.

Where personal information is compromised there may be an impact on the following:

- Individuals - whose information has been put at risk;
- Staff - whose actions placed the information at risk. Such staff may have breached local policy, and this could potentially lead to disciplinary action. There may also be legal implications and potential criminal action taken if they have breached key legislation.
- Organisations - whose actions placed the information at risk. Such organisations may experience a lack of trust confidence or reputation from the public and potential prosecution under information legislation.

Guidelines for transferring personal information are included below however wherever an employee is unsure of the most appropriate method for transmitting personal data they should consult the Council's Information Governance Team. Wow Zone, the contracted IT consultants may also be able to provide secure solutions for regular or bulk transfers of personal information.

Email

Personal information may only be sent by Aspects Care email to another aspectscare.co.uk email address. Where it is necessary to send personal or otherwise confidential information to an email address outside Aspects Care network this must be done using a secure email tool.

Staff may not email Aspects Care information to their personal email accounts. However, staff may email their own personal information to themselves at their own risk, for example a copy of their online payslip, but they must not forward any information they have access to as part of their job to their personal email account.

If you regularly send personal information to a particular public sector organisation such as the NHS, Department of Work and Pensions, the Police or another Local Authority there may be more efficient ways to safely email between organisations, such a squirrel net, etc.

SFX

Where there is a need to send personal information to an email account which is not on the Public Service Network, for example gmail or hotmail, this must be sent by SFX.

SFX set up, managed and monitored by the Aspects Care IT Support Company Wow Zone Ltd.

The SFX system will send an encrypted email and it is necessary to agree a password with the recipient before the email is sent to them.

Post – Internal and External

Wherever possible documents should be scanned, and the electronic copy sent by email or other secure electronic means.

Internal Post

Services Personal information sent by internal mail must always be in a sealed envelope and addressed to a named recipient. Where the information is sensitive, the envelope should be protectively marked.

Care should be taken when re-using envelopes to ensure any previous address is properly removed or obscured to avoid the correspondence being sent to the old address by mistake.

Where the contents relate to an employee's personal life rather than their work (for example occupational health issues or their pension) ensure the envelope is clearly marked 'Private & Confidential'.

External Post

Postal and courier services can be used to transfer personal information either in paper format or as electronic information on removable media.

An assessment of the risk posed by sending personal information by post or courier must always be carried out in order to decide whether it is appropriate to use these methods. The following should be considered, and a senior manager consulted should there be any doubt:

- The nature of the information, its sensitivity, confidentiality or value.
- The damage or distress that could be caused to individuals if the information was lost or stolen.
- The effect any loss would have on Aspects Care

There are a number of standard requirements which must be adhered to when transferring information by post or courier services:

- Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel.
- Mark the envelope/parcel, private and confidential and add on return address details where this will not compromise confidentiality.
- Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit.
- Consider use of an approved courier, registered post or other secure mail method which can be tracked and is signed for.
- Electronic information on USB stick or hard drive being sent by post or courier, must be encrypted prior to transfer.
- Couriers must be made aware of the sensitivity of the contents and any delivery instructions – for example ‘do not leave with neighbours’ or ‘return to sender if unable to deliver’. These instructions should be confirmed with the courier service in advance.

Fax

Always consider alternatives to faxing personal information - for example secure email or delivery by courier. **Fax should always be a last resort!**

Where it is absolutely necessary to fax personal information, the following measures must be taken:

- Telephone the recipient of the fax let them know that you are about to send a fax containing confidential information.

- Ask if they will wait by the fax machine whilst you send the document.
- Ask if they will acknowledge the receipt of the fax.
- Check the fax number you have dialled and check again that it is correct before sending.
- If this fax machine is going to be used regularly, store the number in your fax machines memory.
- Request a report sheet to confirm that the transmission was O.K.
- Do not leave the fax on the machine when it has been sent.
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential. Please see below for suggested wording.

Suggested wording for fax cover sheet:

The information contained in this fax is STRICTLY CONFIDENTIAL and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately. Thank You

When sending personal information by fax you must not:

- Send faxes where you know that the information will not be promptly collected by the intended recipient
- Send faxes at times that maybe outside the recipient's hours of work
- Leave information unattended whilst a fax is being transmitted

Transporting Data by Hand (Paper and Electronic)

Wherever possible data should be transferred by secure electronic means such as secure email.

However, there may be occasions when it is necessary for an employee to transport information outside of Aspects Care 'by hand', whether in paper files or on a portable electronic device. In all such cases these rules must be followed:

- Wherever reasonably practical original files should not be removed from the Aspects Care's offices/systems - instead a copy of the original information should be taken.

- Only the minimum information necessary for the task may be transported. Copies of full files must not be used if only a small section is required.

- A record must be kept of all original documents which are taken outside the Aspects Care. Enough detail must be recorded to ensure we would know what had been lost if it went missing or was destroyed.

- Information should be de-personalised, as far as practical, in order to limit the damage if it were to be lost or stolen. Any details which are not necessary should be removed. For example, a staff member making regular visits to vulnerable individuals may only need a list of the service user's' initials and the time of each appointment rather than a printout titled 'Supported Living Visits' with each customers' name, address, date of birth and telephone number.

- Any electronic device used to transport personal information must have been properly encrypted by the manufacturer or Wow Zone. As well as laptops, tablet computers and smart phones encryption must also be applied to storage devices such as portable hard drives and USB memory sticks. Please note that the use of a log on password or pin number does not necessarily mean that a device is encrypted. If you are unsure whether a device is appropriately encrypted, please consult Wow Zone immediately.

- Staff may not use their personal computer, mobile phone or any other electronic device to store or transport Aspects Care information without the written permission of the Registered Manager. Where the information contains personal data written permission must also be obtained from the HR Manager. Where the information contains health and/or social care information written permission must also be obtained from Aspects Care's Caldicott Guardian.

- Wherever practical, devices or records containing personal information should be returned to company premises at the end of the working day rather than being take home by the employee.

- Where it is necessary for an employee to take a device or records home overnight, they must make all reasonable efforts to keep them safe. They must be stored in a place which is out of sight to visitors; preferably in a locked cabinet or room. The employee must ensure the information is not accessed by any member of their household or person visiting their home.

- Staff using paper diaries or notepads which are taken outside company premises must remove any personal information from them at the earliest opportunity. Any details which need to be retained should be moved onto the relevant paper file or computer system. If the original version is not to be retained on file, it should be securely shredded.

- Where information must be transported by hand all reasonable security measures to protect it must be taken be taken, these should include as a minimum:

    - Devices or records must not be left unattended in public;

    - Devices or records should be transported in secure lockable bags;

    - When using public transport, the employee must not leave the bag containing the records or electronic device unattended on luggage racks but should instead keep it with them; extra care should be taken to remember the bag when getting off the train, bus, hovercraft, air balloon, taxi, etc;

    - Devices or records should not be left in private vehicles but if it is unavoidable, they must not be left where they can be seen – instead they should be locked in the boot or a lockable storage compartment.

- Any loss, theft or destruction of the information must be reported at the earliest possible opportunity. Aspects Care will treat any failure to report lost, damaged or destroyed personal information very seriously in accordance with its disciplinary procedures.

Use of Computers, Internet and Emails

Aspects Care makes computers, computer equipment, internet services and email available to our employees as a business tool to help them perform their job role more effectively. Whilst we acknowledge the benefits that the use of such technology can have for our organisation, it is vital that it is used reasonably, professionally and for appropriate purposes.
This policy sets out rules for the use of computers, email and the internet. The rules in this policy are very important and as such we expect them to be complied with at all times. A serious violation of this policy may result in summary dismissal for gross misconduct.

Personal Use

We permit employees to use company computers and internet services or emails for the purposes of browsing the internet and sending or receiving personal email. Aspects Care does permit social media sites to be accessed.

Personal use is only permitted e.g. during break times and providing it does not interfere with the operational needs of Aspects Care. Personal use is subject to the rules set out in the rest of this policy.

You should not use our computer systems, internet services or company email account for any matter you wish to be kept private from Aspects Care.

Security

The security of our systems and data is of great importance to Aspects Care. If it is compromised it could harm our business or expose it to the risk of harm. To prevent this from occurring, you are required to comply with the security measures detailed below.

Unauthorised software

Software other than that provided by Aspects Care is not to be downloaded or installed onto company computers unless specifically authorised by your manager.

External devices and equipment

No external devices or equipment should be attached to our computers or computer equipment without the prior approval of your manager.

Computer viruses

Whilst Aspects Care has anti-virus software and spam filters in place, it is still expected that employees will take reasonable care to ensure that our systems do not become infected. If you are suspicious that an email or an attachment may have a virus, you should not open it. You should report it to your manager immediately.

If you become aware of a virus or any other programme in our computer system that could cause harm, whether to the computer system itself, its security or our data, you must report this immediately to your manager.

Confidential Passwords

Passwords are confidential and must not be given to another person without prior permission from your manager. If you are preparing to leave your position with this Company for any reason (for example because you have resigned), you must immediately make any passwords used in the course of your employment known to your manager.

Securing your computer terminal

You are required to secure your computer terminal if you are leaving it unattended. You must either log off or lock your system. This is to maintain the security of our systems and data.

If you are using a laptop computer or any other mobile computing device it is your responsibility to ensure that it is kept secure at all times. Particular care must be taken whilst away from the workplace. All mobile computing devices must be password protected. When it is not actively in use, you must switch off or lock your device to prevent unauthorised access being gained to our systems or data. In the event of loss or theft of a device, you must report this immediately to your manager.

You are permitted to use memory sticks to store information when it is required by your role or by Aspects Care. Any information stored on a memory stick must be secure; this means it must be e.g. password protected with a strong password, encrypted. You are responsible for ensuring that the memory stick is not lost or stolen whilst in your possession.

If loss or theft does occur, you must immediately report this to your manager and provide a description of the information on the device.

Modification of Company Equipment

You must not make any modifications to computer equipment or computer software (including removing software) without first obtaining permission from your manager.

Use for Prohibited Conduct

Aspects Care's computers and computer equipment are provided for the legitimate business purposes of this Company. As such, their use for prohibited conduct will be treated very seriously and may result in your dismissal without notice. The examples of prohibited conduct detailed below are non-exhaustive.

Aspects Care strictly prohibits the use of our computers, computer equipment, office equipment, email or internet systems to access, view, create, post, download, store, send, print, copy or distribute:

- Illegal material;
- Pornographic material of any kind or material of a sexual nature;
- Obscene material;
- Discriminatory, defamatory, harassing, derogatory or insulting material;
- Offensive material (that is material likely to cause offence, upset or embarrassment if it is received, seen or discovered to have been accessed);
- Confidential material unless authorised to do so.

The following actions are also prohibited:

- Generating or otherwise participating in the distribution of a virus;
- Copying software;
- Using company programs and software for any unauthorised use;
- Using company software or design programs for unauthorised use;
- Uploading, downloading, opening or distributing unauthorised software;
- Infringing the trademark and/or licencing rights of this Company or any other individual or organisation;
- Infringing the copyright of any individual or organisation.

Email Usage

Aspects Care recognises that email is a useful business tool. However, it is crucial that it is used in a professional manner at all times. All employees are required to comply with the rules set out below. At no time should email be used for Prohibited Conduct.

Appropriate use of email

You should correspond by email only when it is appropriate for you to do so. In any email sent in the course of employment you must ensure that:

- The tone and content is appropriately professional,

- You identify yourself in an appropriate manner;
- You include Aspects Care's standard disclaimer.

Confidential information

You are responsible for ensuring that you do not use email to reproduce, replicate, duplicate or distribute confidential company information to an inappropriate party.

You are strictly prohibited from transferring confidential information to your personal email account.

Creating contractual commitments

It is important to remember that contracts and contractual obligations can be created by email. You must not create a contract or any contractual obligations with a third party unless it is Aspects Care's intention to do so and you have the appropriate authority. If you require further information regarding this, please contact your manager.

Use of emails in court proceedings

Emails can be disclosed in legal proceedings. You must bear this in mind when drafting, responding to or forwarding emails. Even if emails are deleted, it is likely that they are recoverable and as such capable of being disclosed.

Group emails

If you are sending a group email to service users or healthcare professionalsyou must ensure you protect the confidentiality of our service user list and the privacy of service users and potential service users.

Jokes

Using email for the receipt and distribution of jokes and banter is not permitted. Email is one of the least secure methods of communication. What may seem like a joke to you may be offensive to someone else.

Junk mail (spam) and chain emails

Sending and responding to junk email chain letters/emails is forbidden.

Political and charitable donations

You are prohibited from using email to request or respond to a request for political or charitable donations.

Managing your email account

It is your responsibility to ensure that you have sufficient space in your 'Inbox' to enable you to receive emails at all times. You should regularly electronically archive old emails to ensure that your email account is able to function efficiently.

You must use the ‘out of office’ function on our email system when you are out of the office. If you are unsure who to forward your emails to in your absence, contact your manager. The ‘out of office’ message received by those who contact you must be professional. It should include the following information e.g. the date/time when you will next be contactable and who will be dealing with your emails in your absence.

If necessary for business purposes, Aspects Care may access your emails in your absence.

Internet

Aspects Care provides internet access as a tool to assist employees to perform their roles. It must be used in a reasonable and professional manner at all times.

You must not engage in any Prohibited Conduct, or act in a manner which breaches any company policy or term of this handbook. It should be remembered that ‘cookies’ and similar tracking devices may be left on website visits and these can be traceable to Aspects Care. As such you must not visit any websites or carry out any activity on the internet which would be inappropriate in a business environment.

If, as part of your role you are permitted to make ‘postings’ (or carry out similar actions) on the internet on behalf of Aspects Care, you will receive additional guidance from your manager regarding what is and what is not acceptable to Aspects Care.

Any breach of this part of the policy will be treated seriously and may result in your dismissal.

Aspects Care reserves the right to block access to any website it deems inappropriate for employees to access using its systems.

Watching live television on the Internet

This Company does not hold a television licence. As such you are strictly prohibited from watching or recording live television at our premises using our equipment.

Internet gambling

At no time are employees permitted to use Aspects Care’s computers, computer equipment or internet to participate in on line gambling of any kind.

Password Protection

General password construction guidelines are used for various purposes at Aspects Care, i.e. user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins). It is important that everyone be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password can be found in a dictionary (English or foreign)

- The password is a common usage word such as: Names of family, pets, friends, co-workers, fantasy characters, computer terms and names, commands, sites, companies, hardware, software, birthdays and other personal information such as addresses and phone numbers.

- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. Any of the above spelled backwards. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$ %^&*()_+|~-=\`{}[]:";'<>?,./)

- Are at least eight alphanumeric characters long.

- Are not a word in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password protection standards

Change passwords at least once every 3 months.
Do not write down passwords

Do not store passwords on-line without encryption.

Do not use the same password for Aspects Care accounts as for other non-Aspects Care access (e.g., personal ISP account, on-line banking, email, benefits, etc.).

Do not share Aspects Care passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Aspects Care information.

Don't reveal a password over the phone to ANYONE

Don't reveal a password in an email message

Don't reveal a password to the boss

Don't talk about a password in front of others

Don't hint at the format of a password (e.g., "my family name")

Don't reveal a password on questionnaires or security forms

Don't share a password with family members

Don't reveal a password to co-workers while on vacation

Don't use the "Remember Password" feature of applications (e.g., Groupwise, Instant Messenger, Internet Explorer, Mozilla).

If someone demands a password, refer them to this document or have them call the HR manager.

If an account or password is suspected to have been compromised, report the incident to IT security and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by security personnel. If a password is guessed or cracked during one of these scans, the incident will be documented, and the user will be required to change their password.

Information Labelling and Handling

Aspects Care GDPR Information Labelling and Handling Policy contain rules for everyone who handles information for the company.

Those who are within the scope of the policy must follow the advice in order to keep the company information securely and comply with that set standards.

What is Processed Information?

Information or data is processed whenever information is indexed, classified, stored, recorded, disseminated, published, copied, organised, amended, retrieved, viewed, disclosed to others, deleted, destroyed, transferred, transmitted, declassified: it is difficult to say there is any activity directed towards the data, which does not amount to processing.

Code of Practice

Labelling and Handling Requirements for All Information

All information must be conspicuously labelled with its Security Classification.

Aspects Care managers are responsible for making sure all information is labelled with its Security Classification. Files must be marked with the highest security level that has been given to any item of information in that file. Information that is not

specifically labelled will be considered to have a classification of “Not Protectively Marked”.

Most information handled by the company is classified as “PROTECT” and is available only to a controlled number of people. More sensitive or valuable information might be classified as “RESTRICTED”.

Acquisition and Creation

When information is acquired or created, it must be given its Security Classification and handled appropriately for that Security Classification and additional particular requirements In every area of the company, it is the responsibility of all managers for that area to see to this.

Many particular requirements exist under the law, company standards and policies. For example, there are important requirements set out in the Data Protection Act; Aspects Care Ltd Monitoring Systems and the Internet and Email Policy. Managers must make themselves and their teams familiar with all the particular requirements of their own business areas.

Storage

All information used to conduct the company business must be recorded in a filing system: this applies to all media, whether it is electronic, paper, photographs or other. All filing systems should have a:

1. Security Classification based on the Information Security Classification Standard,
2. retention schedule and
3. Data protection registration where personal data is contained in the database.

Managers are jointly and individually responsible for deciding and agreeing the Security Classifications and retention dates in their own business area.

Information must be stored appropriately for its Security Classification. For example, paper information classified as “PROTECT” or “RESTRICTED”, should be locked away in cupboards.

Storage of Information not owned by the Company

When anyone stores information on any company equipment, this must only be done in the course of authorised work for the company. For example, those who use the company equipment may not store on any company computer drive copyrighted films or music which they have acquired for a purpose not connected with Aspects Care Ltd authorised work.

This restriction does not apply to information automatically stored by the system without the intervention of any user, as a result of permitted personal use of email or the Internet. The

Managers should follow the Company Information Security policy within the GDPR Policy.

The company reserves the right to monitor and investigate any information stored on its systems, including information stored as a result of personal use of email or the Internet. The company also reserves the right to discard any information stored on company equipment as a result of personal use of the company systems.

When third party-owned personal information is stored on the company equipment merely in order to facilitate the transfer information onto third party equipment, the party who provides that information will be responsible for its security unless there is an express provision otherwise.

For example, if a home worker stores their private home email address on a company owned laptop, in order to send work home, the company is not responsible for the subsequent loss or misuse of that email address, except by express contractual provision.

Storage of information on Equipment not owned by the Company

When information owned by the company is stored on equipment not owned by the company, the information must still be handled in accordance with the company policies, statutory duties and in compliance with any contractual provisions. For example, there are non-disclosure and access restrictions on information Processed by workers who work from home on their own equipment.

Storage of aggregated de-personalised data about ethnic origin, religion, criminality, etc.

Aggregated and de-personalised information, such as sensitive personal information about ethnic origin, must be stored separately from the personal information to which it relates; but if the sample size is very small, it should not be stored at all because it can be traced to individuals.

Access

Access to company business information should be role-based and not individually-based this means that a person can access information classified as “RESTRICTED” or “PROTECT”, in the course of their work, only if their job or role within the company justifies this. Information should not be kept where only one individual can access it.

Information

Everyone who accesses information must have security clearance and their identity should be checked.

No data should be accessed remotely but must always be accessed from Company-owned machines connected directly to Company-managed networks from equipment within Company premises.

Remote Access

Information which is not connected to the network can sometimes be accessed remotely by permission if conditions are met as set out in the Flexible and Remote Working Policy.

Mailbox Labelling and Handling

Emails are always classified as “PROTECT” or “RESTRICTED”, regardless of their content. See the company Email Policy.

The company digital systems, information security policies, procedures and security arrangements are mostly intended to protect information contained in the computer systems. Much of the security is handled automatically by the system, but there will always remain vulnerabilities to various threats - viruses; hackers who invade wireless networks, etc. Therefore, always comply with the general security rules that protect the system, even when handling Not Protectively Marked (unclassified) information.

An individual responsible for the use of system data must always be identifiable in the system. Never reveal your password or share passwords and user identities; always log out of systems when the session is idles For example, if you access a case management system, you must enter the same user identity and password formalities, whether you are at a hospital site or somewhere else on the Aspects Care Ltd network.

Access to non-system information - portable prints, copies and portable data generally

Portable information is contained in hard copy (paper, photographs, microfiche, maps etc) or on portable media (for example memory sticks, CD’s, laptops, mobile telephones, Blackberries, palm held devices, cameras etc.). Access to portable information will not usually be audited or authenticated automatically, and therefore it is important to label, authorise, and maintain the audit trail.

1. Labelling

Portable information must be labelled with its security classification, and possibly with extra labels such as “personal” or “confidential”. For example, investigation paperwork should be labelled RESTRICTED and should contain a note “If lost or stolen Return to Head Office. File names can be a useful place to put the label in electronic portable data, for example, a CD could contain a file named

“SecurityInvestigationRESTRICTEDdeleteApril2023”

Access must then be restricted appropriately: for example, extracts or details of audit investigations (classified as “RESTRICTED”) should not appear on the lower classification Service Desk logs (classified “PROTECT”).

2 Authorisation and responsibility for portable information.

Copied information classified as “PROTECT” or “RESTRICTED”, must always be the responsibility of a particular person. It is a manager’s responsibility in each business area to decide what portable handling needs to be specifically authorized, and what is understood by a team as being generally allowed without the requirement for specific authorization. Managers must make sure this is clearly understood in their area of the business. Where there is no specific authorization required, labelling and handling responsibilities rest with the person who uses and transports the portable information.

If “RESTRICTED” information is converted to any portable format and removed from the workplace for any reason, (for example, printed out and taken to an external meeting), there should be one person who agrees to take custody and responsibility for looking after it safely. If nobody takes responsibility by agreement, then the handler who printed it, is responsible. If you are handing “RESTRICTED” information to someone else who then becomes responsible for it, make them sign a receipt for it and keep the receipt as part of an audit log or you remain responsible.

3. Audit log

All portable use of RESTRICTED information should be recorded in an audit log.

Use

Information must be used in compliance with company policy and statute and ensure particular importance is the Data Protection Act, which contains rules about handling personal information.

Rules for the Physical security of information classified “PROTECT” or “RESTRICTED”.

1. When you discuss information classified “PROTECT”, “Confidential” or “RESTRICTED”, in public places, take care to keep the conversation from being overheard and take care what information is left on answering machines.
2. Copied information on memory devices such as memory sticks, CDs, telephones or iPods should only be downloaded onto processing equipment which is approved by the company and meets minimum connection standards.
3. Portable information must be physically secured and must not be left unattended For example, do not leave it in a parked car; wherever possible hold and guard laptops and information storage devices personally; if you are the person responsible, store storage devices wherever you judge it is most secure. If information is lost or stolen, the person who is handling it at the time it was stolen must inform Director of services straight away.

4. You should take care to position your screen when viewing information classified “PROTECT”, “Confidential” or “RESTRICTED” on a computer, so that it is difficult for others to see, particularly if your workplace is accessible to the public. You should remove information promptly from view after use.

5. Do not leave prints and copies lying around. Collect copies from copiers and scanners immediately.

6. Rooms and cupboards containing information classified “PROTECT”, “Confidential” or “RESTRICTED”, and also processing equipment for such information, need to be locked. Security perimeters should be protected by controlled entry gates, reception desks or locks. All information on servers must be kept in dedicated secure rooms protected by locks and individual door fob devices/keys/codes must be allocated only to a controlled group of people authorized to access information servers.

7. Unattended equipment must have appropriate protection – terminate active sessions when you leave your screen

Retention

A retention schedule contains details about the different types of records held in a business area and how long they should be kept. Whenever possible, records should state the retention period in summary filing information. The HR Team review and monitor the paper archived records.

Backup and Archiving

All information held on the company network is backed up regularly as part of an automated process. However, information held on local drives, portable media and paper will need to be backed up locally.

If information is no longer required for current business, but cannot be destroyed, it should be archived, either electronically or physically. Company systems are archived regularly but separate arrangements must be made for information held locally.

Monitoring Systems

Use of our computers and IT systems (including internet and email) are monitored. This also includes personal use of them.

Information obtained by monitoring may be used as part of disciplinary, capability or other company procedures set out in this handbook.

All members of staff should be aware that their use of Aspects Care computing equipment may be monitored. This monitoring may be automated or targeted.

Although the technical solutions to enable monitoring may be available to staff, no monitoring will ever be permitted because it is technically possible. All monitoring will be justified on the following grounds only:

Automated Monitoring

Aspects Care may undertake automated monitoring for the either of the following purposes:

- The effective and efficient planning and operation of IT facilities
- The detection, mitigation and prevention of cyber threats

Where automated monitoring reveals activity which Aspects Care cannot reasonably be expected to ignore, the matter will be referred to HR Manager who will decide whether the matter should be shared with enforcement agencies or whether authorisation for targeted monitoring should be obtained.

Targeted Monitoring

Non automated (targeted) monitoring may be undertaken if criminal activity, which the University cannot reasonably be expected to ignore, is detected as a consequence of automated monitoring. If a student is alleged to have engaged in such activity, the University may report them to the police who will determine the nature and scope if any subsequent investigation.

Non automated (targeted) monitoring of IT facilities and systems issued to, and used by, staff members will only be undertaken to the extent permitted by or as required by law and as necessary or justifiable for the following purposes:

- Detection and prevention of infringement of these and other policies and regulations
- Investigation of alleged misconduct
- Handling email and other electronic communications during an employee's extended absence
- To find lost messages or to retrieve messages lost due to computer failure
- To comply with any legal obligation

Filtering

Staff wishing to view material on external websites whose access has been disabled by targeted filtering should refer to Wow Zone who will organise how access can be

granted, and any material acquired as a result should be stored. No attempt should be made to circumvent the filters without following the procedures.

Data Security

Aspects Care takes the security of personal data seriously. Aspects Care has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

Where Aspects Care engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and Company measures to ensure the security of data.

Data Breaches

On occasion, personal data may be lost, stolen, or compromised. When this happens, the incident must be reported immediately. This is vitally important as people may be put at risk of harm and quick action can reduce the potential for damage and distress to the victims.

Any data breach incident will be assigned to an investigating officer who will in most cases be senior member of the service in which the breach occurred.

The investigating officer will ensure the incident is contained, arrange for all necessary parties to be informed and ensure appropriate measures are taken to reduce the risk of similar incident in the future. In order to assist with this please provide the following when reporting an incident:

- What data is involved?
- What format it is in and whether it is encrypted or otherwise protected?
- Who is affected, what type of information and how many records?
- How sensitive is the information?
- Are there any potential risks to individuals?
- What steps have already been taken to recover/locate the information?
- If items have been stolen, please ensure the incident has been reported to the police and provide the crime number.
- What actually happened and which employees were involved?
- Details of any ongoing, immediate risk to information security.

If as a result of an incident, they have concerns for any person's immediate safety they must make all reasonable efforts to warn them straight away.

Aspects Care may also need to report the breach to the ICO within 72 hours. A data breach is any incident involving the loss, damage, inappropriate disclosure or inappropriate access to Aspects Care information or unauthorised access to Aspects Care's data systems. Such incidents can lead to identity fraud or have other significant impacts upon individuals and must be treated very seriously.

A data breach can involve electronic or paper records or the verbal disclosure of details held in our systems or records.

Loss of Electrical Equipment

The use of remote location monitoring should be used wherever feasible to track/ locate the devise as quickly as possible.

Where the breach involves the loss of electrical equipment wherever possible the piece of equipment should be remotely “wiped” to remove data from it.

All electrical equipment should be used in line with Information Governance and Information Security policies.

Confidential Waste Disposal

Confidential waste is defined as waste that contains personal data or data that is considered sensitive to the Aspects Care’s business. For example:

a. Personal data, as defined by the Data Protection Act 2018.

b. Finance information e.g. payroll, pensions or benefits.

c. Staffing information e.g. personnel files, occupational health records.

d. Commercially sensitive e.g. contracts, maintenance records. e. Service user information e.g. care records.

e. Any information classified as Official or Official-Sensitive

It can be produced in a number of formats manual and electronic, paper, audio and video recordings, microfiche, photographs, image files, databases, CDs, DVDs, computer hard drives, removable data storage.

Confidential waste bins are bins provided by Aspects Care for the sole purpose of storing paper-based confidential waste.

Data is the reinterpretable representation of information in a formalised manner suitable for communication, interpretation or processing e.g. a number, word or symbol in a report, spread sheet or database.

Aspects Care will destroy confidential waste to eliminate or erase it beyond any possible reconstruction.

Confidential Waste Disposal Procedure

This procedure applies to all Aspects Care buildings and locations.

This procedure applies to all confidential waste held by Aspects Care, regardless of format. This includes documents and records in electronic or digital form as well as physical form (hardcopy).

Aspects Care will ensure that:

a. Confidential waste is disposed of in accordance with relevant legislation and statutory requirements.

b. Information, data and records that are no longer required will be appropriately disposed of.

c. All those working for or on behalf of Aspects Care will be made aware of the need to dispose of confidential waste securely and in accordance with this Procedure.

It will do this by ensuring:

1. Paper confidential waste will be collected from Aspects Care buildings in line with the contractual requirements of the waste disposal firm.

2. Where possible, small volumes of paper confidential waste can be shredded using a shredder which conforms to DIN P- 4 as a minimum.

3. Prior to collection, paper confidential waste will be stored in bags in a secure location, with access restricted to only those with a business need to access it.

4. Paper confidential waste will be collected and transported only by the contract firm.

5. Where paper confidential waste is not collected by courier, all confidential waste must be shredded before disposal.

6. Confidential waste stored electronically (e.g. on a hard drive) will be disposed of via the Finance Team.

Employees and departments will do this by complying with the following:

1. Review any waste to assess if it should be considered confidential waste.

2. Paper documents will be placed in confidential waste as soon as they are no longer serve a business purpose.

3. Confidential waste should not be left unattended when not in a secure location.

4. Where confidential waste has been disposed of incorrectly (e.g. put in standard recycling) attempted recovery should be processed via the HR Manager.

Destruction of Electrical Equipment

The objective of the approach taken by Aspects Care is to ensure:

- Compliance with WEEE Directive (Waste Electrical and Electronic Equipment) through appropriate disposal of IT equipment.

- Compliance with Data Protection Act 1998 through secure disposal of personal data which states:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

This includes:

- Deletion of confidential or sensitive non-personal data to avoid breach of confidence, breach of contract, commercial damage.

- Deletion of software which is under licence to avoid breach of licences.

- Aspects Care recovers any residual monetary value of IT equipment where appropriate.

It is Aspects Care's policy that:

- No IT equipment (including portable devices) may be disposed of other than by Director of Services via the processes set out in this policy. Users with equipment which needs to be disposed of should contact Director of Services to ensure the safe disposal of the equipment.

- All IT equipment must be disposed of in accordance with Aspects Care's Waste

Management Policy.

- Prior to the disposal of computer equipment, all personal and sensitive data must be securely destroyed by a method appropriate to the risk associated with the sensitivity of data and the equipment on which it is stored as set out in the table below.

- All other data and any software licensed to Aspects Care is removed prior to the equipment leaving the possession of Aspects Care.

- If IT equipment is disposed of by third party contractors on behalf of Aspects Care, they must adhere to the relevant standards and provide the relevant certificates of destruction and copies of waste consignment notes.

Disposal of IT Equipment

Director of Services should be notified of any IT equipment which is no longer required. The Director of Services will then ensure the equipment is reused or disposed of as appropriate. When disposing of equipment, the Director of Services will ensure the deletion of any data and the correct disposal of equipment in accordance with this policy.

The Aspects Care operates a risk based approach which differentiates disposal techniques based on the user of the IT equipment and the type of data it is likely to contain, as outlined below:

Item	Data/Use	Risk	Proposed Method of data destruction	Reasons
PCs and Laptops	Standard office use on managed desktop and student PCs	Low	Overwriting drive multiple times	Low risk of relevant data being on PC in the first place Efficient in terms of volume of equipment, staff time, physical space
	Regularly used for processing personal data or sensitive personal data e.g. HR, Finance, Senior Managers	Medium	Overwriting drive multiple times	Relevant data is likely to be present, therefore need for security outweighs operational efforts required. Will ensure data is effectively not recoverable. Data on laptops should be encrypted so if recovered will still be encrypted.

	Used for processing non-personal confidential or commercially sensitive data	High	Physically destroy	Impact of data loss high, could lead to court action, severe reputational damage and loss
Servers	Storage of personal data, sensitive personal data and confidentiality of commercially sensitive data	High	Physically destroy	Large volumes of data. Mix of personal, sensitive personal, confidential, commercially sensitive data. Disks are not in practice resold but are reused in other systems until they fail or become obsolete
Other Portable devices	CDs, USB sticks (pen drives), floppy disks, memory cards, tapes	Medium	Physically destroy	Simplest and most secure option. With CD-Rs there is no option to overwrite For CD-R should be undertaken as soon as the data is no longer needed to be stored in that way. For other removable media should be undertaken when the storage device is no longer needed.

	Larger USB drives, and external hard disks.	Medium	Overwriting drive multiple times	Relevant data is likely to be present, therefore need for security outweighs operational efforts required. Will ensure data is effectively not recoverable.

Moving PCs

It is common practice for PCs to be moved between individuals and between Directorates and Faculties during their lifetime at Aspects Care. There are two risks associated with this practice:

- There is a risk that if a PC has been used for illegal purposes by one user, evidence of that activity will remain on the PC when it is transferred to a new user. This makes it unclear in any investigation as to who is responsible for any illegal activity.

- New users may have access to confidential or personal data which had been previously stored on the PC.

In order to mitigate this risk, it is Aspects Care policy that all PCs are data wiped when being permanently transferred from one individual to another.

Multi-Function Devices, Photocopiers and Printers

Multi-function devices, photocopiers and printers have hard disks on which electronic copies of documents which have been photocopied, printed, or scanned are stored during the operation of the device. Such hard disks must have their data removed by either data wiping or physical destruction which is dependent upon the level of risk associated with the device when it is decommissioned. As part of the contractual arrangements with suppliers, the Aspects Care is provided with proof of data destruction when the device is returned on termination of the lease.

Smart Phones

All smart phones must have their data removed by being reset to factory default or by physical destruction dependent on the level of risk associated with the device and the data it has held when the device is decommissioned. If a device cannot be reset to factory default due to hardware malfunction, then it must be physically destroyed.

Portable Media

Portable media which has, or had in the past, contained confidential and personal data should be disposed of in accordance with the above table.

Sale of IT Equipment

Where IT equipment has a residual value Aspects Care may choose to resell equipment if it is cost effective to do so. All sales will be undertaken in accordance with Aspects Care's waste disposal policy and the WEEE directives. All sales must be agreed by Director of Services.

Sub-Contractor Agreements

Any individuals officially appointed to work on behalf of or sub-contracted by Aspects Care must abide by the principles outlined in this policy and the data protection charter.

Specifically, they must ensure that:

- All personal data collected and processed for and on behalf of Aspects Care by any party is collected and processed fairly and lawfully;
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s);
- All personal data is accurate at the time of collection; Aspects Care must keep it accurate and up to date while it is being held and/or processed;
- No personal data is held for any longer than necessary in light of the stated purpose(s);
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- Data is not unnecessarily duplicated or distributed;
- Data protection risks will be considered and mitigated by carrying out a Data Protection Impact Assessment in certain circumstances.

No personal data is transferred outside of the UK without first ensuring that appropriate safeguards are in place in the destination country or territory.

Aspects Care shall ensure that the following measures are taken with respect to the processing of personal data utilised accessed or processed by sub-contractors:

- A designated data protection officer (DPO) within Aspects Care shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the legislation.

- All subcontractors will be made fully aware of both their individual responsibilities and Aspects Care's statutory responsibilities and shall be either provided a copy of this policy or directed to a copy available on the Aspects Care's website.

- All subcontractors who process personal data will be appropriately trained to do so.

- All subcontractors who process personal data will be appropriately supervised.

- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed, and internal data audits carried out at least every three years.

- All subcontractors who process personal data will be bound to do so in accordance with data protection legislation and this Policy by contract. Failure by an employee to comply shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply shall constitute a breach of contract. In all cases, failure to comply may also constitute a criminal offence under data protection legislation.

- All subcontractors, agents, consultants, partners or other parties working with Aspects Care who process personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Aspects Care arising out of this Policy and data protection legislation. Aspects Care may carry out due diligence on all external parties prior to engagement to seek assurances in respect of compliance with data protection legislation.

- Where any subcontractor, agent, consultant, partner or other party working with Aspects Care fails in their obligations under this Policy that party shall indemnify and hold harmless Aspects Care against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

- Upon terminating service to Aspects Care all subcontractors, consultants, partners or other parties working on behalf of Aspects Care warrant that they have returned and destroyed all duplicate copies of any personal data they have held whilst undertaking activities on behalf of Aspects Caret and will not

use, retain or transfer any such information collected whilst in the services of Aspects Care.

- Upon terminating services to Aspects Care all subcontractors, consultants, partners or other parties working on behalf of Aspects Care will have their work email account and access to Aspects Care network terminated with immediate effect.

- A data subject must inform Aspects Care in writing if they wish to exclude their personal data from particular data processing provisions contained within this Policy, being mindful that complete exclusion would result in the individual being unable to continue as a sub-contracted employee.

Subject Access Requests

An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information.

We must provide an individual with a copy of the information they request, free of charge. This must occur without delay, ideally within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month.

We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

Freedom of Information (FOI) Requests

The FOI Act will only apply to Aspects Care as a private sector business if

the information Aspects Care share with a public body is subject to an FOI request.

The information Aspects Care shares is published under the public body's publication scheme.

Information Governance

Aspects Care is commissioned to deliver healthcare services for the NHS and Local Councils and as part of its contractual requirements it must ensure that it complies

with the objectives prescribed in the NHS Mandate and to uphold the NHS Constitution.

This policy is important because it will help the staff who work for NHS and social services to understand how to look after the information, they need to do their jobs, and to protect this information on behalf of service users.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards. It provides a consistent way for staff to deal with the many different information handling requirements including:

- Information Governance Management
- Clinical Information assurance
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary use assurance
- Respecting data subjects' rights regarding the processing of their personal data

The formal framework that leaders of all health and social care organisations should commit to is set out in the National Data Guardian's ten data security standards. These are the basis of the Data Security and Protection Toolkit that Aspect Care uses to assess its information governance performance.

Under data protection legislation, because Aspects Care processes personal data it is accountable for and must be able to demonstrate its compliance with the legislation. The arrangements set out in this and related policies and procedures are intended to achieve this demonstrable compliance.

Purpose

The purpose of this policy is to inform Aspects Care staff (permanent or otherwise) of their Information Governance responsibilities and the management arrangements and other policies that are in place to ensure demonstrable compliance.

This is the central policy in a suite of policies that informs staff of what they should do:

To maximise the value of organisational assets by ensuring that Aspects Care demonstrates data is:

- Held securely and confidentially
- Processed fairly and lawfully
- Obtained for specific purpose(s)
- Recorded accurately and reliably
- Used effectively and ethically, and
- Shared and disclosed appropriately and lawfully

To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental Aspects Care will ensure:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained, and tested
- Information governance training will be available to all staff
- All information governance breaches, actual or suspected, will be reported to, and investigated by the Senior Management team in conjunction with the Data Protection Officer

Scope

All our staff and any subcontractors, without exception, are within the scope of this policy, including and without limitation:

- Senior Management Team
- Registered Managers and Head Office Care Staff
- Finance Team
- HR and Administration Team
- Support Workers
- Training Officer

Roles and Responsibilities

Director of Care

Overall accountability for procedural documents across the organisation lies with the Director of Care as the Accountable Officer that has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements, and adhering to guidance issued in respect of information governance and procedural documents.

Caldicott Guardian

The Human Resources Manager has been appointed Caldicott Guardian.

They will:

- Ensure that Aspects Care satisfies the highest practical standards for handling service user identifiable information
- Facilitate and enable appropriate information sharing and make decisions on behalf of Aspects Care following advice on options for lawful and ethical processing of information, in particular in relation to disclosures
- Represent and champion Information Governance requirements and issues at Senior Management Team level

- Ensure that confidentiality issues are appropriately reflected in Aspects Care's strategies, policies and working procedures for staff
- Oversee all arrangements, protocols, and procedures where confidential service user and/or staff information may be shared with external bodies both within, and outside, Aspects Care

Senior Information Risk Owner (SIRO)

The Director of Care has been nominated as Senior Information Risk Owner (SIRO) for Aspects Care. The responsibilities of the SIRO are:

- Take overall ownership of the Aspects Care's Information Risk Policy
- Understand how the strategic business goals of Aspects Care, and how other organisation's business goals may be impacted by information risks, and how those risks may be managed
- Implement and lead the Information Governance Risk Assessment and Management processes within Aspects Care
- Sign off and take accountability for risk-based decisions and reviews in regard to the processing of personal data
- Advise the Senior Management on the effectiveness of information risk management across Aspects Care
- Receive training as necessary to ensure they remain effective in their role as SIRO.

Data Protection Officer

The Data Protection Officer (DPO) is the Human Resources Manager, who reports to the SIRO, but also can act independently of the SIRO and report directly to the Senior Management Team about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations regarding potential changes to, or new initiatives that, involve processing of personal data. With the support of their office, the DPO will:

- provide advice to Aspects Care and its employees on compliance obligations with data protection law
- advise on when data protection impact assessments are required
- monitor compliance with data protection law and organisational policies in relation to data protection law
- co-operate with, and be the first point of contact for the Information Commissioner
- be the first point of contact within the organisation for all data protection matters
- be available to be contacted directly by data subjects

- consider information risk when performing the above

Information Asset Owners

Information Asset Owners (IAOs) will:

- Lead and foster a culture that values, protects and uses information for the benefit of service users
- Know what information comprises or is associated with their asset(s) and understand the nature and justification of information flows to and from the asset
- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy
- Understand and address risks to the asset and provide assurance to the SIRO
- Ensure there is a legal basis for processing and for any disclosures
- Refer queries about any of the above to the Director of Care
- Ensure all information assets they are owner for are recorded in the Information Asset Management Ledger and maintained
- Undertake specialist information asset training as required

Head of Information Governance

The Head of Corporate Information Governance will be the Director of Care and s/he will:

- Maintain an awareness of information governance issues within Aspects Care
- Review and update the information governance policy in line with local and national requirements
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis
- Ensure that line managers are aware of the requirements of the policy
- Work with the Caldicott Guardian, SIRO and DPO functions to ensure organisational authority and awareness regarding issues relating to data protection or confidentiality concerns.

Head of ICT Technology and IT Cyber Security

The Head of ICT Technology and IT Cyber Security is the Human Resources Manager, and that individual has responsible for developing, implementing, and

enforcing suitable and relevant information security procedures and protocols to ensure Aspects Care's systems and infrastructure remain compliant with data protection legislation.

The Human Resources Manager is responsible for ensuring that all Aspects Care electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

Director of Services

The Director of Services is responsible for:

- The formulation and implementation of ICT related policies and the creation of supporting procedures, ensuring these are embedded within the service and developing, implementing, and managing robust ICT security arrangements in line with best industry practice
- Effective management and security of Aspects Care's resources, for example, infrastructure and equipment
- Developing and implementing an IT Recovery Plan
- Ensuring that ICT security levels are met
- Ensuring the maintenance of all firewalls and secure access servers are always in place, and
- Acting as the Information Asset Owner for the ICT infrastructure with specific accountability for computer and telephone equipment and services that are operated by staff, e.g. personal computers, laptops, personal digital assistants and related computing devices, held as an company asset.

Line Managers

Line managers will take responsibility for ensuring that the Information Governance Policy is implemented within their group or directorate.

All Staff

It is the responsibility of each employee to adhere to this policy and all associated information governance policies and procedures. Staff will receive instruction and direction regarding the policy from several sources:

- DPO office
- Corporate Information Governance Team
- Policy/strategy and procedure manuals
- Line manager
- Specific training course
- Other communication methods, for example, team meetings; and

- Staff intranet

All staff are mandated to undertake mandatory information governance related training in line with the training needs set out by Aspects Care Senior Management Team, including GDPR.

Information governance training is required to be undertaken on an annual basis by all staff.

All staff must make sure that they use the organisation's IT systems appropriately and adhere to the use of Emails, Internet and Computers Policy.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc. of personal data, states it is an offence for a person knowingly or recklessly:

a) to obtain or disclose personal data without the consent of the controller

b) to procure the disclosure of personal data to another person without the consent of the controller, or

c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

Information Governance Policy Framework

Aspects Care has developed a framework for their Information Governance Policy. This is supported by a set of Information Governance policies and related procedures to cover all aspects of Information Governance which are aligned with local Council contractual Information Governance requirements and the NHS Operating Framework and the Data Security and Protection toolkit requirements.

Many of these proposals are supported by underpinning procedures. The Staff Handbook provides a brief introduction to Information Governance and summarises the key user obligations that support the Information Governance policies and procedures. The Staff Handbook must be read, and the declaration accepted by every member of staff during induction.

Information Governance External Support

Aspects Care has secured the services of an external HR consultancy service which includes the provision of expert advice and guidance to managers on all elements of Information Governance.

The External Support offered relates to:

- Providing advice and guidance on internal Information Governance
- Managing the delivery of improvement plans to meet DSP Toolkit assertions.
- Developing internal IG policies and procedures
- Reviewing IG training programmes for staff
- Ensuring compliance with Data Protection, Information Security and other information related legislation
- Providing support to the team who handle freedom of information requests

- Providing support to the Caldicott Guardian and Senior Information Risk Owner (SIRO) for internal Information Governance related issues.

The Human Resources Department is responsible for:

- Liaison with strategic external stakeholders
- Providing support advice and guidance to internal strategic projects and programmes
- Leading on the scoping, commissioning, quality assuring and where appropriate providing Information Governance advice and guidance
- Working with the Senior Management Team to ensure there is consistency of Information Governance across Aspects Care and to establish protocols on how information is to be used (including sharing)
- Working with external stakeholders to ensure consistency of information governance standards and requirements across the health and social care system.

Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Human Resources Team, on a periodic basis.

The Director of Care is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

Confidentiality of Information

Any information obtained during the course of a member of staff's employment relating to Aspects Care, its business, proposed acquisitions, financial details, products, reports, suppliers, customers, personnel, service users and all matters is (with the exception of information made public by Aspects Care) confidential

Similarly, any information gained about our service users is to be considered as highly confidential and, as with confidential information about Aspects Care Ltd itself, must not be disclosed directly or indirectly to any other individual, body, firm or company either during or after your employment with Aspects Care.

Only if information about our service users is in the public domain (and we have to be sure that we're right if we think this) or unless we have the express written permission of the service user to divulge the story or piece of information, may we talk about the issue to others.

Be particularly careful when naming or writing about other service user in a report, paper, article or course where they could potentially be identifiable. The written word stays around for a lot longer and is a lot more 'discoverable' than the spoken word. Act professionally with Aspects Care Ltd interests in mind whenever considering using written referral of one service user to another. Be particularly careful where Aspects Care Ltd might be the ones responsible for putting a service users

confidential information into the wider public domain (e.g. in an article, or in a conference presentation).

Responsibilities – Offices

Aspects Care offices house all current details relating to our service users and business. It is anticipated that staff will use these facilities on a regular basis and interruptions will occur. It is necessary, therefore, to have regard for other staff and not misuse this office as a meeting place.

Visitors entering the building are requested to sign in via the visitor's book and are requested to use the seating facilities in the main office area, please receive your guests as soon as possible and accompany them. They will be issued with a visitor's badge, which they must display prominently at all times whilst on the premises.

Staff should consider other staff and stagger lunch breaks if possible. Office based staff are required to take their half an hour break in/around the middle of the working day. The Main Offices are managed over the lunch period, but for the security of all it would be beneficial to have someone else in the building. Ensure someone within each department is always available during break times.

Although Aspects Care Ltd is flexible on dress and appearance, staff should be dressed smartly and professionally at all times.

In order to create and maintain an environment free from smoke in which people can work in maximum comfort and without risk to their health or safety, smoking is not permitted on company premises.

Responsibilities – Out of Office

Aspects Care reputation relies not only on our care and support capabilities but also on its ability to satisfy different service users' demands as regard our behaviour as individuals.

Aspects Care is building its reputation as a professional company that understand that the needs of service users are as important as the care and support provided. As such – our personal relationships with service users – when away from the main office are vital and there is an expectation on all staff to understand this and act accordingly.

When in the service users' home then due care should be given to respect for privacy and dignity. Whilst out with a service user during the day, at night, during meals, on journeys, or undertaking an activity then their wishes and thoughts should be taken into account at all times.

Certainly, any complaint from service users about the unsuitability or unprofessionalism of our behaviour will be thoroughly investigated as a matter of the utmost seriousness and may render the individual(s) concerned subject to disciplinary action.

During work time ‘smart-casual’ is the minimum dress standard – even where local dress-code may be ‘casual’. Only in exceptional circumstances should this rule be relaxed. When with service users and you are attending a specific event/occasion then due consideration to the type of event/occasion being attended should be given and the mode of dress should reflect this.

Aspects Care makes its reputation on being seen as professionals who have genuine empathy with their service users. Politeness and courtesy at all times are the expectation. Staff should never allow their guard to drop and never discuss matters which breach the boundary of the staff/service user relationship.

During the course of any shift the rule is absolute – no consumption of alcohol is permitted. Staff cannot imbibe alcohol or any drinks containing alcohol no matter how small a percentage. When the service user they are supporting wish to attend a public house as part of their general activities or if a service user wishes to drink in their home, staff must ensure they drink non-alcoholic drinks only. All staff need to keep in mind that they are there in a care/support role and have responsibilities towards their service user which alcohol intoxication could impair. Any member of staff found to be drunk or to have consumed any alcohol whilst with a service user or on standby on call for a service user will be subject to the disciplinary procedure.

Our service users rely on our confidentiality. NEVER discuss confidential matters with other service users or individuals - and always be VERY mindful of being overheard inadvertently (say at night between meal tables, or, say, on trains). Aspects Care reputation may be seriously damaged by any instance of real or perceived breach of confidentiality and any such occurrence will render the member(s) of staff concerned liable to the most severe disciplinary action.

NEVER discuss matters of internal confidentiality to Aspects Care the presence or earshot of service users or their representatives. Be particularly mindful of this when using mobile phones.

Staff should refrain from using case-studies or stories where other service users may be identifiable. There may be incidents or events which practically illustrate specific issues – but must never breach the confidentiality of service users in doing this. Such incidents and events must either be suitably ‘sanitised’ or the relevant service users must have given written permission to reveal the information to others. If in doubt – staff should not reveal the information and another way of making the point should be used. These restrictions shall continue after your employment has been terminated.

If staff are using incidents/events or case studies where names are used, the recipient audience should always be explicitly reassured that such information has been approved to be used because it’s information either in the public domain or that we have to express permission to use (which must, of course, then be true) These restrictions shall continue after your employment has been terminated.

Aspects Care gain nothing from actually or potentially being seen to be disparaging with regards to other organisations or individuals who are competitors. As such,

Aspects Care have a rule to NEVER get dragged into this sort of situation. No member of staff should knowingly disparage other organisations or individuals to an external source.

Confidential information, in whatever format made or received by you during the course of your employment is our property.

You must return to us, on our request or upon termination of your employment, any confidential information which belongs to us and is in your possession or under your control. You must delete, on our request, all confidential information in your possession and destroy any other documents and/or items which are in your possession or under your control and which contain or refer to any confidential information.

You must not retain any copy/copies of any confidential information belonging to us. At any time during your employment, or following termination of your employment, we may require you to provide a written undertaking that you have returned all property belonging to us including confidential information and that you have not retained any copy/copies of confidential information belonging to us.