**Data Protection and GDPR Policy**

1. **Purpose**
   1. Omega Care Grouphave this policy in place to ensure adherence to data protection and GDPR. This policy sets out guidelines and appropriate working practices to ensure compliance. Further to this, this policy also sets out a standardised response to any reported data breach incident and ensure that data breaches are appropriately logged and managed in accordance with the law and best practice.
2. **Scope**
   1. This procedure has been written in line with the GDPR Government guidelines. It applies in the event of a personal data breach and applies to all employees of Omega Care Group.
   2. The policy is applicable to all services operated by Omega Care Group.
   3. GDPR applies to all information we holdand all information technology systems utilised byus.
3. **Responsibility**
   1. All employees (including bank staff), contractors and third parties working for or on behalf of us must adhere to this policy and are required to be aware of, and to follow this procedure in the event of a personal data breach.
   2. All employees (including bank staff), contractors and third parties working for or on behalf of us are responsible for reporting any personal data breach to the Managing Director.

**4. Introduction**

Everyone working in the home has a responsibility to ensure that personal information collected on young people within Omega Care Group is stored securely, and that when it is shared with other agencies this is done appropriately and in accordance with the law.

The Data Protection Act 2018 and the General Data Protection Regulations (GDPR) provide a framework to ensure that personal information which is collected and processed by organisations is done so fairly and lawfully, that it is accurate and relevant, stored securely (for no longer than necessary) and that, when it is shared, this is done appropriately and lawfully.

When working with children and families, effective sharing of information is essential for the early identification of need, to complete robust assessments and to provide services which are tailored to individual need.

Keeping children safe from harm will require staff in all provisions and others to be proactive and share the following types of information:

* Any concerns they have about the safety or welfare of a young person; and
* Any adults with whom a child is having contact which may impact on the young person’s safety or welfare.

Information sharing is also essential for the identification of patterns of behaviour; for example when a young person has gone missing and when multiple children appear associated to the same context or locations of risk (this would include for example, concerns around trafficking, Child Sexual Exploitation and Child Criminal Exploitation).

Often, it is only when information from a number of sources has been shared and is then put together, that it becomes clear that a child has suffered, or is likely to suffer, significant harm.

No staff should not assume that someone else will pass on information that they think may be critical to keeping a child safe. Anyone who has concerns about a young person’s welfare and considers that they may be at risk, has suffered or is likely to suffer significant harm, should share their concerns with the young person’s social worker and / or the Police.

Staff should use their professional judgement and knowledge from training when making decisions about when to share information. If staff have any concerns or doubts, the home's manager or safeguarding lead should be consulted for advice.

**5. The Legal Framework**

* The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between homes, Children's Social Care, the Police and other local agencies (such as schools), will be essential for keeping children safe and ensuring they get the support they need.
* The overarching principle set out in the GDPR and the Data Protection Act 2018 is that any personal information cannot be shared with another person / organisation unless either: the young person providing the information (or their parent / carer if the young person does not have sufficient age and understanding) has consented to their information being shared; or
* The disclosure / sharing is necessary to safeguard the welfare of a child, young person or adult at risk, in which case the public interest in protecting children and at adults at risk permits the sharing of personal information without consent.
* Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety of, children which must always be the paramount concern. The GDPR and Data Protection Act 2018 are not barriers to sharing information, where the failure to do so would cause the safety or well-being of a child to be compromised. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns. The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child or young person.

This includes:

* + Disclosure of potential or actual harm of self
  + Disclosure of potential or actual harm to other
  + Disclosure of potential or actual harm of others to others

In the case of Children in Need, Child Protection or children/young people at risk of significant harm, it is difficult to foresee circumstances where the law would be a barrier to sharing personal information with other practitioners.

([Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (DfE)](https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice)).

Staff should therefore feel confident that information can be shared even without consent if to gain consent would place a child (or vulnerable adult) at risk, or the sharing is necessary to safeguard the welfare of a child or adult at risk, in which case the public interest permits the sharing of information.

Whenever information is shared, it must be done securely and in accordance with any relevant local policies. In addition sharing should always be proportionate (meaning only relevant / key information is shared).

**6.**  **Key Points for employees when Sharing Information**

Wherever possible you should be open and honest with the child / young person (and/or their family where appropriate) from the outset as to why, what, how and with whom their information will be shared;

* Seek advice from other practitioners (such as your manager or safeguarding lead) if you are in any doubt about sharing the information concerned, this should be done without disclosing the identity of the individual where possible;
* Where possible share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the Data Protection Act 2018 and GDPR, you may still share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so;
* Sharing should always be necessary, proportionate, relevant, accurate, timely and secure: Ensure that the information you share is necessary for the purpose for which you are sharing it, that it is shared only with those people who need to have it, that it is accurate and up-to-date, that it is shared in a timely fashion, and that is shared securely (Staff should always follow the home's policy for handling personal information);
* Keep a record of your decision and the reasons for it - whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Source: [Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (DfE)](https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice).

Informing Children about Disclosure

Young People should be informed of the circumstances in which information about them will be shared with other professionals and their consent to this sharing should be sought. This information may be provided in the form of a Young Person Induction Pack, a Privacy Notice or in other ways, and it will be made clear that in each case the information passed on will only be what is relevant and on a 'need to know' basis.

**7. Sharing Information with other Professionals to Provide the Best Possible Support**

Sharing relevant information promptly with others working with the same child is central to safeguarding the young person’s interests and to ensuring they receive the best possible care. Staff should work in partnership with other professionals involved in caring for the young person (for example, education, social workers, health professionals and youth justice) to monitor the young person’s progress, share information and obtain expert advice as appropriate. Therefore, relevant information about young person must be shared with colleagues, other professionals or agencies who have a role to play in their support or need the information in order to look after the young person.

Where information is requested by telephone or electronically, great care must be taken to ensure that the recipient is entitled to receive the information requested. Where there is any doubt the information may not be provided without the approval of a Manager.

When staff are not certain regarding the identity of the individual requesting information staff should seek relative information of the individual. This will include requesting the child or young person’s full name, legal status, DOB and social worker. Staff should also seek confirmation with the social worker prior to sharing information.

**EMPLOYEE PRIVACY NOTICE**

Omega Care Group is committed to protecting the privacy and security of your personal information and we will always treat you and your data with the respect you deserve.

This Privacy Notice covers how we collect, use, store and disclose the data that you supply to us and your rights about data that we hold about you. It applies to current and former employees, workers, volunteers, interns and contractors and does not form part of any contract of employment or other contract to provide services. For more information please contact the Data Protection [manager/ officer/individual - Tony Mathewson] who will provide you with our Data Protection Policy.

**THE INFORMATION WE COLLECT FROM YOU**

Personal individual 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 will collect, store, and use the following categories of personal information about you:

**PC** - Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

**DOB** - Date of birth.

**G** - Gender.

**MSD** - Marital status and dependants.

**NOK** - Next of kin and emergency contact information.

**NI** - National Insurance number.

**FI** - Bank account details, payroll records, travel logs and expenses and tax status information.

**EB** - Salary, annual leave, pension and benefits information.

**SD** - Start date.

**WL** - Location of employment or workplace.

**DVLA** - Access to your DVLA portal.

**RI** - Recruitment information (including copies of right to work documentation, passport, references and other information included in a CV or cover letter or as part of the application process).

**ER** - Employment records (including job titles, work history, working hours, training records and professional memberships).

**COM** - Compensation history.

**PER** - Performance information.

**DG** - Disciplinary and grievance information.

**CCTV** - CCTV footage and other information obtained through electronic means such as swipe card records.

**ICS** - Information about your use of our information and communications systems.

**P** - Photographs.

We may also collect, store and use “special categories” of more sensitive personal data which require a higher level of protection:

**HR** - Information about your health, including any medical condition, health and sickness records (including Occupational Health records).

**A** - Absence notes.

**ED** - Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.

**TU** - Trade union membership.

**GI** - Genetic information and biometric data.

**CC** - Information about criminal convictions and offences.

**How the information is collected**

We collect personal information through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers or other background check agencies [credit reference agencies] We may collect additional personal information in the course of job-related activities throughout the period of you working for us.

**When we will use your personal information**

We need all the categories of information identified above primarily to allow us to perform our contract with you [\*\*\*\*\*\*\*\*\*] and to enable us to comply with legal obligations [\*\*]. In some cases, we may use your personal information to pursue legitimate interests of our own or those of third parties [\*\*\*] (provided your interests and fundamental rights do not override those interests). We will process your personal information as follows, the asterisks show the purpose for processing:

|  |  |  |
| --- | --- | --- |
| Purpose | Type of data | Lawful basis |
| Making a decision about your recruitment or appointment. | PC, RI, ER | \*\*\* |
| Determining the terms on which you work for us. | EB, SD, PC, RI, ER | \*\*\* |
| Checking you are legally entitled to work in the UK. | PC, DOB, NI, DVLA | \*\* |
| Paying you and, if you are an employee, deducting tax and National Insurance contributions. | PC, NI, FI, SD | \*\* \* |
| [Providing the following benefits to you: [optical examinations] | PC, DOB, G, MSD, NOK, NI, FI, EB, SD | \* |
| Liaising with your pension provider. | PC, DOB, NI, EB, SD | \* |
| Administering the contract, we have entered into with you. | PC, NOK, NI, FI, EB, SD, WL, PER, DG, ED | \*\*\* \* |
| Business management and planning, including accounting and auditing. | PC, DOB, G, NI, FI, EB, SD, WL, PER, DG, ICS, HR, ED, TU | \*\*\* |
| Conducting performance reviews, managing performance and determining performance requirements. | PC, EB, SD, WL, PER, DG, CCTV, ICS, ED | \*\*\* \* |
| Making decisions about salary reviews and compensation. | PC, FI, EB, SD, WL, RI, ER, PER, DG, CCTV, ICS | \*\*\* \* |
| Assessing qualifications for a particular job or task, including decisions about promotions. | PC, RI, ER, PER, DG, ED | \*\*\* \* |
| Gathering evidence for possible grievance or disciplinary hearings.  Making decisions about your continued employment or engagement. | PC, PER, DG, CCTV, ICS, ED  PC, PER, DG, CCTV, ICS, ED | \*\*\* \* |
| Making arrangements for the termination of our working relationship. | PC, NI, FI, EB, PER, DG, ED | \*\*\* \* |
| Education, training and development requirements. | PC, ER, PER, DG, ED | \*\*\* \* |
| Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work. | PC, FI, EB, COM, PER, DG, CCTV, ICS, P, HR, A, ED, GI | \*\*\* |
| Ascertaining your fitness to work and managing sickness absence. | PC, DOB, G, MSD, NOK, WL, PER, DG, CCTV, ICS, P, HR, ED | \*\*\* \* |
| Complying with health and safety obligations. | PC, NOK, WL, ED | \*\* \* |
| To prevent fraud. | PC, NI, FI, DVLA, RI, ER, GI | \*\*\* |
| To monitor your use of our information and communication systems to ensure compliance with our IT policies. | PC, CCTV, ICS | \*\*\* |
| To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. | PC, CCTV, ICS | \*\*\* |
| To conduct data analytics studies to review and better understand employee retention and attrition rates. | PC, DOB, G, MSD, HR, ED | \*\*\* |
| Equal opportunities monitoring. | PC, DOB, G, MSD, HR, ED | \*\*\* |

Please refer to our Data Protection Policy, in the Team Handbook which provides more detail on how we collect your data, the basis on which we hold it and how we store, use and destroy it.

**Failure to provide information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing employee benefits), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

**SENSITIVE PERSONAL INFORMATION**

“Special categories” of particularly sensitive personal information require higher levels of protection. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal obligations and in line with our Data Protection Policy.

3. Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme], and in line with our Data Protection Policy.

4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

**Our obligations as an employer**

We will use your particularly sensitive personal information in the following ways:

1. We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
2. We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
3. We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
4. We will use trade union membership information to pay trade union premiums, register the status of a protected employee and to comply with employment law obligations.

**INFORMATION ABOUT CRIMINAL CONVICTIONS**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our [data protection policy].

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

We envisage **OR** do not envisage that we will hold information about criminal convictions and access your DBS portal.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

1. Complete a DBS risk assessment

We are allowed to use your personal information in this way to carry out our obligations [SPECIFY] **OR** [SET OUT ANOTHER LAWFUL BASIS].

**Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current, so please let us know if your information changes.

**DISCLOSURE/DATA SHARING**

We may have to share your data with third parties, including third-party service providers (including contractors and designated agents); other entities in the group; in the context of a sale of the business; or with a regulator or to otherwise comply with the law; our insurers and/or professional advisers to manage risks legal disputes. [The following activities are carried out by third-party service providers: [payroll, pension administration, benefits provision and administration, IT services] **OR** The following third-party service providers process personal information about you for the following purposes: [NAME PROVIDERS AND THE ACTIVITY THEY CARRY OUT]].

We do this where required by law; where it is necessary to administer the working relationship with you; or where we have another legitimate interest in doing so.

We require third parties to respect the security of your data and to treat it in accordance with the law.

**Transfers of data outside of the EU**

We may transfer the personal information we collect about you outside the EU in order to perform our contract with you. We use Microsoft SharePoint which covers our email servers and cloud-based file storage system, further information is available from the person responsible for Data Protection in our Company.

**DATA RETENTION**

We must store most of your HR data for a period of at least 6 years following the termination of your employment; some personal financial data will be destroyed after 2 years; Health and Safety information must be held for a minimum of 40 years.

**YOUR RIGHTS**

**Your rights in connection with personal information**

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

1. **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. Please refer to our DSAR Procedure for more information.
2. **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
3. **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
4. **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
5. **Request the restriction of processing** of your personal information. 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.
6. **Request the transfer** of your personal information to another party.

**Right to withdraw consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Please contact the person responsible for Data Protection in our Company.

**COMPLAINTS & QUESTIONS**

If you have any questions about this privacy notice or how we handle your personal information, please contact the person responsible for Data Protection in our Company. If we have breached our duty of care, we will take appropriate action.

If you are not satisfied by our response you also have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues (**Email**: [casework@ico.org.uk](mailto:casework@ico.org.uk))

**CHANGES TO THIS PRIVACY NOTICE**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

# Omega Care Group - Data Subject Access Request Procedure

**8. Data Subject Access Request Procedure**

* 1. **Purpose**
     1. Omega Care Grouphave this procedure is in place to provide a standardised response to any data subject access requests (“DSARs”) that we receive and ensure that DSARs are appropriately managed and responded to in accordance with the law and best practice.
     2. Data subjects have the right to request access to their personal data processed by us and are entitled to obtain:
* Confirmation that their data is being processed;
* Access to their personal data;
* Any related information;
  1. **Scope**

This procedure only applies to data subjects whose personal data we process.

For the purposes of this procedure, “personal data” means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. “Processing” means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

* 1. **Procedure** 
     1. If you receive a DSAR direct from a data subject, please forward the details onto the Managing Director. When a data subject makes an DSAR we shall take the following steps:

(a)  log the date on which the request was received to ensure that the relevant timeframe of one month (unless the DSAR is found to be excessive) for responding to the request is met;

(b)  confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;

(c)  search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d)  confirm to the data subject whether or not personal data of the data subject making the DSAR are being processed.

If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

(a)  the purposes of the processing;

(b)  the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

(c)  the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

(d)  where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e)  the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f)  the right to lodge a complaint with the Information Commissioner’s Office (ICO);

(g)  where the personal data are not collected from the data subject, any available information as to their source;

(h)  the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i)  where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

We shall also, unless there is an exemption (see below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

Before providing the personal data to the data subject making the DSAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

If the DSAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

If we are not going to respond to the DSAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

* 1. **Exemptions**

Before responding to any request, we shall check whether there are any exemptions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with a DSAR to safeguard:

(a)  national security;

(b)  defence;

(c)  public security;

(d)  the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e)  other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

(f)  the protection of judicial independence and judicial proceedings;

(g)  the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h)  a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in Paragraph 4.1(a) and Paragraph 4.1(g) above;

(i)  the protection of the data subject or the rights and freedoms of others; or

(j)  the enforcement of civil law claims.

* 1. **Document Control**

A current version of this document is available to all members of staff in the office.

This procedure was approved by *Alex Aresti- managing director* on *25.08.2020* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | <Manager> | Xx/yy/zz |
|  |  |  |  |
|  |  |  |  |

1. **Data Breach Notification Procedure**
   1. **Purpose**
      1. Omega Care Group(“we”/”us”)have this procedure is in place to provide a standardised response to any reported data breach incident, and ensure that data breaches are appropriately logged and managed in accordance with the law and best practice.
   2. **Scope**
      1. This procedure applies in the event of a personal data breach and applies to all employees of Omega Care Group at all times and whether located within the physical offices or not
      2. The document applies to all information we holdand all information technology systems utilised byus.
   3. **Responsibility**
      1. All employees/Staff, contractors or temporary employees/staff and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.
      2. All Employees/Staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Managing Director contact details are as follows:

Name: Alex Aresti

Telephone: 07920048141

Email: [a.aresti@omegacaregroup.org](mailto:a.aresti@omegacaregroup.org)

* 1. **Definition**

The GDPR defines a “personal data breach” in Article 4(12) as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. Examples include:

* Loss or theft of data or equipment on which data is stored
* Access by an unauthorised third party
* Sending personal data to an incorrect recipient
* Alteration of personal data without permission
* Loss of availability of personal data such as equipment failure
* Unforeseen circumstances such as a fire or flood
* Hacking attack
* ‘Blagging’ offences where information is obtained by deceit for the purposes of this procedure data security breaches include both confirmed and suspected incidents.

\*If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach please refer the matter to the Managing Director for consideration\*

* 1. **Reporting an incident**
     1. Any individual who accesses, uses or manages information within our business is responsible for reporting data breach and information security incidents immediately to the Managing Director.
     2. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.
     3. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.
  2. **Next Steps**
     1. The Managing Directorwill firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
     2. An initial assessment will be made by the Managing Director in liaison with relevant persons (which may include IT services) to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).
     3. An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered/reported.
     4. The Managing Director will investigate the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
     5. The Managing Director will then establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
     6. The Managing Director will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.
  3. **Procedure – Breach notification data processor to data controller**
     1. Omega Care Group must report any personal data breach or security incident to the data controller without undue delay.
     2. The breach notification should be made by email and telephone.
     3. A confirmation of receipt of this information should be requested and made by email and telephone.
  4. **Procedure – Breach notification data controller to supervisory authority**
     1. The Managing Director will determine if the supervisory authority (the Information Commissioner’s Office (ICO) in the UK) need to be notified in the event of a breach.
     2. If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The *Managing Director* will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.
     3. We will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation and/or an impact assessment. If we decide that we do not need to report the breach to the ICO we will justify and document our decision.
     4. If a risk to data subject(s) is likely, the *Managing Director* will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.
     5. If the data breach notification to the ICO is not made within 72 hours, Managing Director will submit notification electronically with a justification for the delay.
     6. If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.
     7. The following information needs to be provided to the supervisory authority:
        1. A description of the nature of the breach.
        2. The categories of personal data affected.
        3. Name and contact details of the *Managing Director*
        4. Likely consequences of the breach.
        5. Any measures taken to address the breach.
        6. Any information relating to the data breach.
        7. Approximate number of data subjects affected.
        8. Approximate number of personal data records affected.
     8. The breach notification should be made via telephone - **ICO: 0303 123 1113.** Alternatively, if the *Managing Director*may choose to [report it online](https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc) if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.
     9. In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register.
  5. **Procedure – Breach notification data controller to data subject**
     1. If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Omega Care Groupwill notify those/the data subjects affected without undue delay and in accordance with the *Managing Director* recommendation.
     2. A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. In any event the *Managing Director* will document their decision-making process.
     3. We will describe the breach in clear and plain language, in addition to information specified in clauses 8.7.1-8.7.6 above.
     4. The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.
     5. If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner and will be considered by the *Managing Director* who’s decision will be final.
     6. If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Omega Care Group will communicate the data breach to the data subject by telephone or email.
     7. We will document any personal data breach(es) within the Data Breach Register, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.
  6. **Documentation requirements**
     1. Internal breach register: there is an obligation for us to document each incident “comprising the facts relating to the personal data breach, its effects and the remedial action taken”.
  7. **Evaluation**
  8. Once the initial incident is contained, the *Managing Director* will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.
  9. Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.
  10. The review will consider various points, including but not limited to:
* Where and how personal data is held and where and how it is stored
* Where the biggest risks lie, and will identify any further potential weak points within its existing measures
* Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
* Staff awareness
  1. **Document Control**

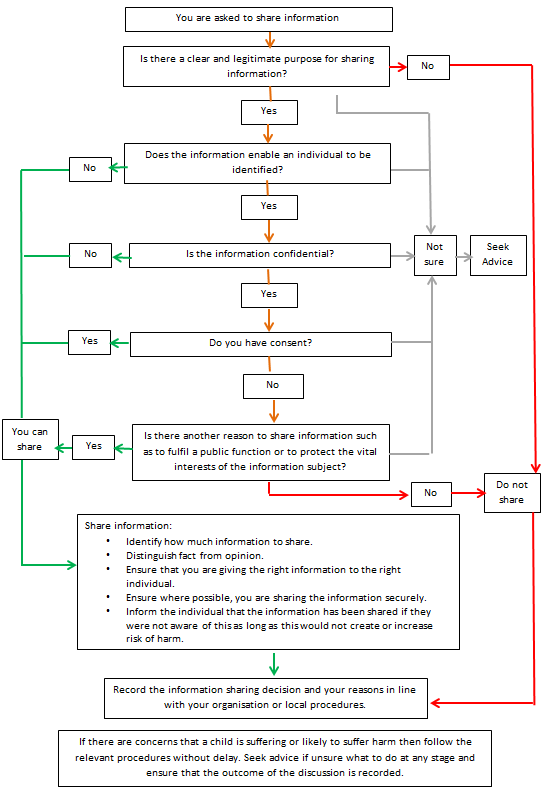
A current version of this document is available to all members of staff in the office.

This procedure was approved by *Alex Aresti* on *25.08.2020* and is issued on a version controlled basis under his/her signature.

Signature: Date:

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Alex Aresti | 25.05.2018 |
| 2 | Review | Alex Aresti | 25.08.2020 |
|  |  |  |  |

****