

Data Protection Policy

Vital Healthcare Group



Finding Your Way Around

Vital Healthcare Compliance Policies	3
1. Key Requirements for Protecting Personal Information	5
2. Data Protection Risk Assessment & Mapping	7
3. Employee Records	7
4. Dealing with Consumers (B2C)	8
5. Direct Marketing.....	8
6. Dealing with Consumers on Behalf of Other Businesses	9
7. Visitors	10
8. Surveillance of People & Property	11
9. Business to Business Relationships.....	12
10. Hardware Containing Customer or Employee Personal Information	12
11. Providing Information to Third Parties	13
12. Rights Relating to Personal Data	13
13. Reacting to a Breach.....	14
Stop & Ask.....	15

Vital Healthcare Compliance Policies

Our Code of Conduct is based on the simple principle that, across the Vital Healthcare Group, in everything we do, we must Do the Right Thing.

This means that we comply with all the legal and regulatory standards that apply to our activities. But it also means more: we will always aim to follow best practice and to act fairly in whatever we are doing.

We each have the obligation to:

Do the Right Thing

- We must Do the Right Thing every day.
- We follow the laws and internal policies and procedures that apply to our jobs.
- We ensure that our actions are consistent with best practice and our own values.
- We take responsibility for our decisions.

Know Our Stuff

- We know our stuff
- We know this Policy.
- We know other laws and internal policies and procedures that apply to our jobs.

Stop & Ask

If we are not sure how to Do the Right Thing, we Stop and Ask. We can always ask for advice from our line manager, management or HR in our business, or the legal team.

Raise a Concern

We must Raise a Concern if we think that something wrong or illegal is happening in our business.

When does this policy apply?

This Policy applies to every business in which Vital Healthcare has a controlling interest (a 'Vital Healthcare Group business').

The directors of each Vital Healthcare Group business must ensure that this Policy is followed in all areas of their activity. In this Policy the term 'director' refers to any company director or any person who sits on the leadership team or management board of the Vital Healthcare Group business in question.

Businesses in which Vital Healthcare does not have a controlling interest should be requested to comply with this Policy or adhere to equivalent standards to those set out here.

What happens if I do not follow this policy?

Compliance with this Policy will reduce the risk of enforcement action against Vital Healthcare Group businesses because of an accidental or deliberate unauthorised release of personal information. It will also maintain the trust placed in Vital Healthcare Group businesses by customers, suppliers and employees.

By following this Policy, Vital Healthcare Group businesses can make safe and effective use of personal information to enhance the services we provide and build even stronger relationships with stakeholders. Therefore the directors of every Vital Healthcare Group business must ensure that this Policy is applied in their own activities.

A deliberate or negligent failure by a director of any Vital Healthcare Group business to comply with this Policy may result in disciplinary action, up to and including dismissal.

How does this policy relate to other Vital Healthcare Group policies?

This Policy adds detail to the section on Protecting Personal Information in our Code of Conduct.

This Policy sits alongside and is complimentary to other Group policies, including our Group Information Security Policy and the Target IT Standards that sit under it.

What areas are not covered?

This Policy does not cover information that does not relate to individual people, even though that information may be commercially sensitive or covered by non-disclosure obligations. For instance, sales numbers, prices, or anonymous commercial statistics might be commercially confidential but are not personal information.

What is covered by this Policy?

This Policy sets out what is required in the following areas:

1. Key Requirements for Protecting Personal Information
2. Data Protection Risk Assessment and Mapping
3. Employee Records
4. Dealing with Consumers (B2C)
5. Direct Marketing
6. Dealing with Consumers on Behalf of Other Businesses
7. Visitors
8. Surveillance of People and Property
9. Business to Business Relationships Key Requirements for Protecting Personal Information
10. Hardware containing Customer or Employee Personal Information
11. Providing Information to Third Parties
12. Rights Relating to Personal Data
13. Reacting to a Breach

In each of these areas, this Policy sets out minimum requirements and guidance on how to meet those requirements. The requirements are compulsory. It is not compulsory to follow the guidance. However, where it is not followed the directors of the Vital Healthcare Group business in question should be able to demonstrate why the approach they have taken is appropriate.

Governance

The Compliance Questionnaire that is issued periodically to all Vital Healthcare Group businesses will include a number of questions on compliance with this Policy. In addition, compliance with this Policy will be audited.

Key terms

Personal information is any information about an individual person from which that person can be identified. For example, an address, bank details and an account number on a spreadsheet next to a person's name is personal information.

Sensitive personal information (also called **special category data**) relates to a person's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, genetic or biometric data (used for identification purposes), sexual life or orientation, commission or alleged commission of a criminal offence or any proceedings for any offence or alleged offence.

Processing is any use or handling of that personal information. For example, taking a person's order over the telephone is processing their personal information.

The person who can be identified from the personal information, and who owns that personal information, is sometimes referred to as the **data subject**.

1. Key Requirements for Protecting Personal Information

Why is this important?

Protecting personal information is crucial to maintaining trust, ensuring compliance with legal and regulatory requirements, and safeguarding the privacy and security of our customers, employees, and other business partners.

What's required?

We must always ensure that personal information is:

- Used fairly for legitimate purposes that we have clearly communicated to the person who the information is about. We must not use it for any purpose other than the reason we have explained.
- Adequate, relevant and not excessive for the use for which it has been given to us.
- Accurate, including by being up to date.
- Used by us in line with the rights of the information owner.
- Kept by us for only as long as we need it in line with our retention rules.
- Kept safe, using a combination of technology and traditional controls, so that we do not give it to someone who should not have it.
- Gathered and processed in line with the minimum controls set out below.
- Not sent (including using a server) outside the EU, Norway, Iceland and Liechtenstein unless the same level of security we would use is in place.

We must always be able to demonstrate to the relevant authority, through a documented decision making process, that we have introduced appropriate measures and controls to ensure that we are complying with these requirements.

We must design the protection of personal data into all of our processes and systems, operating to ensure that data is protected by default in each business in the Vital Healthcare Group.

Minimum controls

- Each business in the Vital Healthcare Group has to understand where personal information is kept within its business. The business has to map the journey of personal information from its collection through to its final destruction, for example by using a flow chart.
- A director must be responsible for managing the implementation of controls to protect personal information and also for reporting back progress to the business's board. Responsibility for day to day management of the measures introduced by the business can be delegated to a more junior manager, though ultimate responsibility will remain with the relevant director.
- It is important to communicate clearly the policies in place and ensure that employees understand their duties by having in place a training plan, which should include regular refresher sessions. Online training is available through Vital Healthcare's Group training platform.
- To ensure ongoing compliance with this Policy, each business must:
 - » Assess its practical and technical security measures protecting personal information;
 - » Ensure staff awareness of requirements about protection of personal information;
 - » Investigate breaches;
 - » Comply with requests for the provision of personal information by the individuals the information is about; and
 - » Use appropriate technology to monitor information, the use of that information and any attacks on or abuse of the processes.
- Controls have to be in place, such as:
 - » A data protection risk assessment;
 - » A data protection policy;
 - » A data retention policy;
 - » A privacy statement on websites;
 - » Data processing agreements with third parties who are sent personal information;
 - » A surveillance camera policy (when surveillance cameras are used);
 - » Online training;
 - » An access request process; and
 - » Data protection impact assessments (when changes are taking place).
- We carefully destroy records when they become out of date in accordance with the business's data retention policy. We use specialist third party service providers to undertake secure destruction of documents – always ask for and retain a certificate confirming that the documents have been securely destroyed.
- The Group Legal & Compliance team maintains a set of template documents which can be used in the preparation of policies, statements, signage and contracts.

Helpful hint

All of these considerations and requirements apply in the event that you use artificial intelligence in respect of personal or confidential business data. You must always check that any use of artificial intelligence only occurs in accordance with the AI acceptable use policy in your business.

2. Data Protection Risk Assessment & Mapping

Why is this important?

An assessment of risks helps determine the controls and practical steps necessary to ensure adequate security measures for the use of personal information.

What's required?

We must take into account the following factors as part of the risk assessment process:

- The nature and extent of the business's premises and computer systems.
- The number of staff in the business.
- The extent of staff access to personal information.
- Personal information held or used by a third party for the business (the business will remain responsible for ensuring that any third party working with personal information from the business has appropriate security).
- The location of servers that the personal data will be process through (both internal and external).
- The nature of any cross-border transfers of personal information.
- The business's intended use of the personal information.

3. Employee Records

Why is this important?

- The most common type of personal information in a business is information that relates to employees, typically held as employee files with human resources teams or managers. Such files will hold employee personal information.
- In some instances, employee records will hold information about health, sexuality, gender, religion or criminal matters.

What's required?

- We keep employee records safe, secure and up to date. Processing of employee personal data commonly arises where the processing is necessary for compliance with a legal obligation, or where the processing is necessary for the performance of the employer/employee contract.
- We clearly communicate the grounds relied on for processing the employee information.
- We carefully destroy old employee records when they become out of date in accordance with our business's data retention policy.
- We keep sensitive personal information especially secure and only allow it to be used with the express consent of the employee (unless the use is to protect the wellbeing of the employee, for example in case of a health incident in the workplace relevant to information held on record).
- We ensure notes of interviews for prospective employees are retained according to local requirements, for example for evidence of compliance with equality requirements.

4. Dealing with Consumers (B2C)

Why is this important?

- If our businesses sell to consumers we are likely to be given personal information about those consumers to enable us to supply our products to them, follow up with after-sales service and, sometimes because they are interested in finding out more about our products and offers.

What's required?

- We only use personal information provided by consumers to carry out the transaction for which they have provided their information; this includes future account management. For marketing purposes, we can generally rely upon a legitimate interest basis for processing customer data (see Section 5 below about use of consumer personal information for marketing purposes).
- We ensure we have a process for transactions over the telephone or via the web to appropriately verify consumer's identity before any consumer personal information is released.
- We comply with any requirements that require us to provide consumers and other users on our websites the right to provide or decline consent for personal data processing.

5. Direct Marketing

Why is this important?

- Marketing is an important area for use of personal information. Businesses can use personal information to telephone or send direct emails and promotional leaflets to consumers about offers and new products.
- A properly maintained consumer database can be a very valuable asset but it is important that our use of such data is in line with our legal obligations.

What's required?

- We must communicate clearly the legal basis we are relying on to the customer at the time their information is collected.
- When carrying out direct marketing, we consider that we have a legitimate interest in using customer data for direct marketing about our products. However, a decision that it is in the Vital Healthcare Group business's legitimate interest to process customer data for direct marketing in any particular case must be documented and agreed by the directors of the Vital Healthcare Group business in question at the relevant time.
- We keep updated records to show that we have communicated all relevant data processing information, including about their legal rights, to individuals whose data we use for direct marketing.
- We have a process to check any purchased contact lists of consumers against public registers where customers may have indicated they no longer wish to receive marketing by telephone, email or mail. We only buy such contact lists from reputable suppliers who have confirmed that the consent to use of personal information has been given by all of those on the list.

- When collecting personal information for marketing, we display wording clearly which explains any sharing of personal information with other named Vital Healthcare businesses for direct marketing purposes and explain how to opt out. Seek advice from the Group Legal & Compliance team if personal information is going to be sold or given to a third party outside the Vital Healthcare Group.
- We must in our emails offer customers a simple option to unsubscribe. Postal marketing must offer a return address to request direct marketing to stop. If a customer objects to receiving direct marketing of any form, immediately take steps to prevent further direct marketing to that customer.

Examples:

Q: I have some really good offers to communicate to customers. I have planned a marketing campaign which will involve sending leaflets and emails to customers. I will send leaflets to all customers and, where I have an email address, an email. Is there a problem?

A: Yes. Your business has a legitimate interest in carrying out direct marketing. However, before relying on that legitimate interest to send any direct postal mail, you need to check that recipient customers have been informed that we consider that we have a legitimate interest to use their data for direct marketing by postal mail. We can do this by providing appropriate information when we collect their data or by including that information in a letter which sets out our policy and their data protection rights.

If you want to do marketing by email, you can do so where a customer has given us their email address when they recently bought something from us. Where they have, you must send them an individual email without anyone else's details, not using the "to" section in open correspondence, explaining clearly who we are and including an "unsubscribe" button. You have to then ensure that action is taken to remove from the list anyone who indicates that they wish to unsubscribe.

6. Dealing with Consumers on Behalf of Other Businesses

Why is this important?

- Sometimes a business customer will re-sell a product supplied by a Vital Healthcare business to a consumer customer. The business customer will provide personal information about the consumer to enable the Vital Healthcare business to supply the product to the consumer directly.
- This personal information does not belong to us and has been given to us only to deliver the product.

What's required?

- We retain personal information in these circumstances only as a legal record of the completion of the delivery to the consumer or for other legal requirements (e.g. safety recall or tax records).
- We ensure we include clauses obliging the reseller and the Vital Healthcare business to comply with relevant data protection laws in the contractual arrangements between the parties.
- If not required for legal purposes, we destroy or return the personal information to the business customer when the reseller arrangement comes to an end.

Examples:

Q: I have received an order from one of our re-seller customers. She is asking me to deliver one of my products to a consumer. The order sets out the name and address of the consumer and explains that the consumer has three teenage children. I know that I have a number of other products which would be ideal for this consumer and the consumer's teenage children. I tell our delivery driver to take some leaflets to the consumer about our other products and how she can contact me about them. This is adding value to the consumer experience, isn't it?

A: No. There was no need for the delivery information to include any reference to the consumer's teenage children. Your re-seller customer has only sent this information so that you can deliver the ordered product to the consumer. You must not use the personal information for any other purpose.

7. Visitors

Why is this important?

- Visitors entering our sites will provide personal information, often as part of our security processes. Our security systems also may monitor what visitors do on our premises via surveillance or monitoring the use of IT networks.
- Additionally, visitors may have access to areas where personal information is stored or being used.

What's required?

- We control access so that visitors cannot see any personal information they are not authorised to see.
- We keep paper records in locked storage and use screen savers or filters so that computer screens are not visible.
- We use clear signage and other notices to make visitors aware of any steps taken to monitor anything they may do while visiting.

Examples:

Q: A number of suppliers visit our office regularly. They are welcomed in reception and then told where to find the sales person they have come to meet. We have an open plan office. A supplier of mine is visiting the office today. As meeting room space is limited, I will meet him at my desk which is in the middle of my team. I will keep my voice down so that we don't disturb my team. This doesn't cause any issue with personal information, does it?

A: It does. You should check to ensure that your team has locked away all personal information. No personal information should be visible on desks. Computer screens should be turned away or filters should be used so that there is no unauthorised access. Ideally, you should arrange the office so that meetings with external parties are held in a place where there is no visible personal information.

8. Surveillance of People & Property

Why is this important?

- Surveillance cameras are an important way to secure premises and protect our people, but used incorrectly they can infringe an individual's rights.

What's required?

- We have in place a surveillance policy that is communicated to relevant employees.
- We ensure that pictures recorded by the surveillance equipment are only ever seen by authorised personnel as those pictures contain personal information.
- We keep a record of who has access to surveillance pictures.
- We keep surveillance camera images in line with local information retention policies.
- We ensure cameras are only directed at Vital Healthcare business premises (not public roads or paths).
- We ensure signs and notices are displayed explaining why surveillance cameras are being used and the name of the business responsible for the surveillance.
- We do not intrude on private areas such as changing rooms or toilets. Recording of sound as well as images is highly intrusive and generally not permitted by regulators.
- We do not use hidden cameras except in very limited circumstances. If you are unsure of the rules, take legal advice.

Examples:

Q: The managing director of my business has received complaints from employees about the conditions in the staff changing rooms. The cleaning company wants to charge more because of all the extra work it has to do to tidy the changing rooms and clean up graffiti about the business written on the walls. The managing director has asked me to install hidden cameras in the changing rooms to find out who is doing the damage. Given the seriousness of the damage, using the hidden cameras is the best way, isn't it?

A: No. Areas such as changing rooms and washrooms are very private areas. Using cameras in such areas, even where damage is occurring, is such a breach of employee information rights that it cannot be justified.

9. Business to Business Relationships

Why is this important?

- Information about businesses might have to be kept secret because of confidentiality obligations owed by one business to another, whether as a supplier, agent or customer. Rules protecting personal information generally do not apply to information about a business but it will apply to personal information we may hold about employees of that business.
- In addition, where we do business with sole traders or partners in a partnership, we are likely to be dealing with their personal information rather than business information.

What's required?

- We assess all types of information used to determine whether it is about a company, an individual running their own business or an employee at a company.
- We apply appropriate procedures in each case.

Examples:

Q: Jan is my contact at one of our suppliers. I have the email address and mobile telephone number to contact him at work. He heads up the customer account management team and has been with that supplier for five years. He is a football fan who is always keen to talk about his local team. I am working on a project to look at whether some of our suppliers might also be interested in buying services from us. I have put Jan's details into a large database we have created, including background information about Jan such as corporate hospitality he might be interested in and where he lives. I don't need to worry about our data protection policy, do I?

A: Yes, you do. Although you know Jan through a business relationship, the personal information I am using belongs to him and he can be identified. You should ensure that any personal information you hold, whether about an employee, customer or supplier, is kept in line with our policy and rules.

10. Hardware Containing Customer or Employee Personal Information

Why is this important?

- Some personal information used in businesses is held on electronic devices, such as a laptop hard drive, mobile telephones or tablets such as iPads.

What's required?

- We ensure that hardware which is to be recycled or electronic goods which have been returned by a consumer, must go through appropriate security processes to ensure that the memory of each device containing the personal information is totally and permanently erased before the device is released to a third party.
- We use third party service providers that permanently remove personal records from electronic equipment when they provide a certificate of destruction. The certificate must be retained.
- Ensure that your IT team complies with the VITAL HEALTHCARE Group Information Security Policy and Target IT Standards.

11. Providing Information to Third Parties

Why is this important?

- Vital Healthcare businesses use third parties to hold and analyse personal information on their behalf. Examples of third parties that use personal information are payroll and other HR related services, mailing houses, IT service providers, website managers and sales or delivery agents.

What's required?

- We must have a written data processing agreement when personal information is sent to a third party for processing.
- We must assess the third party to ensure it complies with relevant data protection laws, has robust IT security policies and controls in place and will agree to audits to check its controls. For long term relationships with third parties, the third party's security compliance should be assessed periodically. Further details are set out in the Vital Healthcare Group Information Security Policy and the Target IT Standards.
- We must not transfer personal information from inside the EU or the UK to outside the EU or the UK except in limited circumstances. If a service provider is going to send personal information outside the EU, advice must be taken from the Group Legal & Compliance team.
- We ensure that if a relationship ends with a third party who handles customer or employee information, all such personal information needs to be returned or certified as having been securely destroyed.

12. Rights Relating to Personal Data

Why is this important?

- Employees, customers and other individuals have a number of rights relating to the personal information that is being kept about them on computer systems and in any paper-based manual filing systems. Third parties can contact us to exercise these rights at any time.
- Breaches of an individual's personal information rights can result in claims for compensation for damage caused and regulatory fines.

What's required?

We must have a process in place to enable a prompt response if an individual:

- Asks what personal information is held about them (including asking for copies of the personal information held).
- Asks for a correction to be made to any incorrect personal information.
- Asks for the deletion of information held on them (commonly known as the right to be forgotten).
- Objects to processing of personal information that is likely to cause or is causing damage or distress.
- Requests the prevention of the use of their personal information for direct marketing.
- Asks for their data to be handed over to someone else.
- Objects to decisions being taken by a computer using their personal information e.g. an automatic decision based on a computer analysis of income, house size and car ownership.

Examples:

Q: A customer has contacted us, in writing, saying that she would like to know about all the personal information which we hold about her. She believes that we have been using her information to send marketing materials to her, without her consent, but are sending the materials to the neighbouring property instead. I am busy and it will take a lot of time to check through the customer's electronic files. I will wait until she writes to me again. Is this OK?

A: No. The customer has information rights which we must respect. One of the rights is to know what personal information we hold about her. You should speak to your line manager immediately so that you can work out how you can provide the right information in the right timescale. You should also check whether the personal information that we hold is correct.

13. Reacting to a Breach

Why is this important?

- Personal information is a valuable asset. Any unauthorised access to personal information is potentially a breach of an individual's rights. Unauthorised access can arise from:
 - » A loss or theft of IT equipment or information;
 - » A breach of physical security;
 - » The uploading of personal information to a website in error;
 - » Personal information being left in an insecure location;
 - » Unauthorised, co-ordinated access (such as hacking) into IT systems; or
 - » "Phishing", where personal information is obtained by deception.

What's required?

- We ensure we have a procedure for reacting to serious losses of personal information in place, which has been communicated to relevant employees, suppliers and contractors. It is recommended that this procedure be prepared in conjunction with your IT colleagues.
- In the event of a breach, the procedure will outline:
 - » That the leadership team member responsible for protecting personal information must follow the procedure to assess the breach's severity by the volume, sensitivity and exposure of the personal information (a template assessment is available from the Group Legal & Compliance team);
 - » That it should be checked whether outside agencies are involved, how third parties are affected and whether the individuals the information is about have been notified; and
 - » To appoint an internal incident response team to manage such incidents. Notify the Group Legal & Compliance team and the Group IT Security team if a breach occurs.
- We must involve Group Legal & Compliance if an assessment indicates that a report to the relevant regulator is required.
- We always report a breach. A failure to do so can lead to claims for compensation and large fines.
- We do not fail to report "near misses" that will not result in formal action. These should still be reported to allow lessons to be learned and help ensure other Group businesses are aware of risks and opportunities to improve.

International Case Study:

Q: My Group business is based in France, and I am going to use an international company to provide payroll services for us. I will have to send them a lot of employee personal information to set up the arrangement. Their account manager has told me that most of their servers are based in the USA, Mexico, and India. I will send a few emails to the payroll services company and attach spreadsheets containing the personal information they need. Does this create a problem?

A: Yes. Before you send personal information to the external third party, you need to ensure that they comply with EU data protection laws and you have to have a data processing agreement in place. You also need to check their IT security controls which might include an audit, by us or a third party on our behalf.

Stop & Ask

If you have a query about the application of this Policy, please contact any member of the Vital Healthcare Group Legal & Compliance team.

You can use the following Freephone numbers to contact SafeCall:

Austria	00800 72332255	Italy	00 800 7233 2255
Belgium	00800 72332255	Luxembourg	00800 28502
Brazil	0800 892 1750	Netherlands	00800 72332255
Canada	1877 59 98073	Norway	00800 72332255
China (China Telecom)	10800 4400682	Poland	00800 72332255
China (China Unicorn)	10800 7440605	Spain	00800 72332255
Czech Republic	00 800 72332255	Sweden	0850 252 122
Denmark	00 80 25 41 90	Switzerland	00 800 7233 2255
Finland (Elisa)	999 800 7233 2255	Taiwan	00801 444460
Finland (Telia Sonera)	990 800 7233 2255	United Arab Emirates	8000 4413376
France	00800 72332255	United Kingdom	0800 915 1571
Germany	00800 72332255	USA	1 866 901 3295
Ireland	1800 812740		

This service is available 24 hours a day, every day of the year.

We can use Safecall's website: www.safecall.co.uk/file-a-report

We can send an email: vitalhealthcare@safecall.co.uk

You will always be supported if you Raise a Concern about a legal or ethical issue. Retaliation against a person who Raises a Concern is prohibited.



**Vital
Healthcare**

Vital Healthcare
Fannin House
South County Business Park
Leopardstown, Dublin 18
D18 Y0C9, Ireland
T: +353 01 290 7000
E: contactus@vitalhealthcare.com
vitalhealthcare.com