Holden Knight Healthcare Ltd

Data Protection Policy

Human Resources v1.2 November 2026 Review Date: November 2026

Data Protection Policy

1. Introduction

This policy governs the use of personal information within Holden Knight Healthcare Ltd so that all of our team members, individual contractors and other workers (Personnel) will have a clear idea of the limits of use of personal information, and where to go for further advice.

1.1 Purpose

This policy lays down the principles for the processing of personal information, whether it relates to team members, suppliers, guests, customers or others. Personal information means any information relating to a living, natural person, who can be identified either directly or indirectly. Processing personal information includes the obtaining, handling, processing, transporting, storing, destruction and disclosure of personal information.

1.2 It is not designed to replace practical advice from the Data Protection Officer. Nor is it intended to provide all the answers to questions concerning the use of personal information in particular areas, such as HR or IT.

1.3 Additional Guidance notes on specific issues (e.g. Subject Access Rights) are also available from the Compliance/Data Management Team or from our DPO

1.4 Summary

Holden Knight Healthcare will use the personal information of individuals fairly, lawfully, transparently and in a manner consistent with its valid business interests and at the same time, respecting the fair and lawful privacy requirements of those individuals concerned.

1.5 Status of this policy

Personnel who process personal information on behalf of Holden Knight Healthcare must adhere to the terms of this policy and any breach will be taken seriously and may result in formal disciplinary action.

1.6 This policy should be read in conjunction with other relevant Policy and Practice documents. Any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with your line manager or the Data Protection Team. Any Personnel who consider this policy has not been followed should raise this matter with their relevant head of his/her function within Holden Knight Healthcare or (if an employee related issue) the HR Team.

2. Governing Principles

2.1 Personal information will be used within Holden Knight Healthcare by its Personnel according to the principles of applicable data protection legislation (the "**DP Legislation**"), meaning the General Data Protection Regulation ("GDPR"), the Data Protection Act ("DPA"), UK GDPR and the Privacy and Electronic Communications Regulations ("PECR"). The principles require that personal information will be:

Lawfulness, fairness & transparency	The DP Legislation seeks to ensure that processing is carried out lawfully, fairly and transparently without adversely affecting the freedoms, interests and rights of the individual concerned. For personal information to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the individual data subject has consented to the processing, or that the processing is necessary for the performance of the contract with the

	individual, for compliance with a legal obligation, the vital interest of the data subject, or the legitimate interest of Holden Knight Healthcare or the party to whom the information is disclosed. Before personal information is passed to third parties, including law enforcement agencies, government bodies, investigators or anyone else, it is important that full consideration is made of the possible data protection implications of doing so. Again, please contact the Data Protection Officer if you have any questions or are in any doubt regarding a particular request.
Purpose limitation	Personal information may only be processed for the specific purposes notified to the individual when the information was first collected or for any other purposes specifically permitted by the DP Legislation. This means that personal information must not be collected for one purpose and then used for another unless the other purpose is also specified.
Data minimisation	Only personal information that is necessary for the purposes specified should be collected. Any data which is not necessary for that purpose should not be collected in the first place.
Accuracy	Information, which is incorrect or misleading or is not accurate. Steps should be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information should be securely destroyed.
Storage limitation	Personal information should not be kept longer than is necessary for the purpose for which it was collected. This means that data should be destroyed or erased from our systems when it is no longer required.
Integrity and confidentiality	We must ensure that appropriate safeguarding measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Individual data subjects may apply to the courts for compensation if they have suffered damage or distress from such a loss. From May 2018 tough new obligations to notify, in certain situations, regulators (and affected individuals) will be introduced if the above-mentioned safeguarding measures fail to protect personal information. It is therefore very important that you immediately report any suspected incident to the Data Protection Officer. The DP Legislation requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction, be it paper-based or in electronic format. Personal data may only be transferred to a third-party data processor (such as a supplier or service provider to Holden Knight Healthcare or a group company or trading entity) if they agree to comply with those procedures and policies, or if they put in place adequate measures. DP Legislation also requires Holden Knight Healthcare to have a written contract in place with all suppliers or service providers who will process their personal information.

Accountability	We must ensure that we are able to evidence that we comply with DP Legislation. For example, that all the above principles have been applied, documentation is up to date, training on data protection and privacy has been completed, and security measures are complied with.

2.2 Compliance with the principles

In order to meet the requirements of the principles, Holden Knight Healthcare will:

- observe the conditions regarding the fair, lawful and transparent collection and processing of personal information;
- meet its obligations to specify the purposes for which personal information is used;
- collect and process personal information only to the extent it is required for Holden Knight's valid business interests and where there is a legal basis for doing so;
- ensure the quality of the personal information used;
- adopt a data retention and disposal policy that includes the length of time personal information is held;
- ensure that the rights of individuals about whom personal information is held can be fully exercised under the respective DP Legislation;
- take appropriate technical and organisational safeguarding measures (which include strict Personnel access controls) to protect personal information including following the guidelines set out in Holden Knight Healthcare's policies and procedures;

2.2 We will ensure that any contractor, agent or other third party who processes personal information on Holden Knight Healthcare's behalf does so under a written contract requiring that third party to:

- only process the personal information in accordance with Holden Knight Healthcare's instructions; and
- take appropriate technical and organisational security measures to safeguard personal information; and
- ensure that personal information is not transferred outside the European Economic Area without suitable safeguards; and
- confirm destruction of all information. This should include paper, electronic and consideration should be given to backup media; and
- which contains additional data processing clauses which are specified in the DP Legislation.

2.3 Responsibility for compliance

Holden Knight Healthcare is a data controller (and, in certain circumstances, also a processor) responsible for complying with the DP Legislation. It is the responsibility of each member of staff to comply with this policy when using personal information relating to team members, customers or others.

2.4 The Data Protection Officer has responsibility for this policy, review, monitoring of compliance and enforcement.

3. LEGAL BASIS

All processing must be lawful, which means that there must be one of the following legal grounds established before processing can take place:

3.1 Consent

When using consent, Holden Knight Healthcare must be able to demonstrate that consent has been unequivocally given, not just implied. Consent cannot apply to children under 13 vis-à-vis online unless the holders of parental responsibility have provided it. Nor can consent be coerced, for example, forced consent as part of a contract. Consent is a valid legal basis for processing of special categories of personal information. Consent must be prominent in any privacy statement:

- freely given, specific, informed and unambiguous
- a clear affirmative action, signifying agreement to the processing of their personal information

3.2 When consent is given in the context of a statement which also concerns other matters, the request for consent needs to be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

3.3 When consent is provided, it must be able to be withdrawn at any time with as much ease as it was originally given. If withdrawn, the information must be erased[1].

3.4 Legitimate Interests

It is always important to demonstrate the necessity for Holden Knight Healthcare to process personal information for its legitimate interests if relying on this legal basis. When using legitimate interests, Holden Knight Healthcare must be able to demonstrate that there are no over-riding risks to the individuals' interests, rights or freedoms.

3.5 Therefore, Holden Knight Healthcare's legitimate interests when weighed up against the risks to individuals must always be taken into account when conducting a data protection impact assessment (required for any new system or process – or a significant change). Similarly, the mitigating measures that are applied need to be documented.

3.6 Contract

When using contract as the legal basis, Holden Knight Healthcare must be able to demonstrate that the necessity of the performance of a contract (or negotiation of a contract) with the individual, for example, employee, supplier or young person[2].

NB - Consent is presumed not to be freely given if it does not allow separate consent to be given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

3.7 Legal Obligation

When there is a statutory obligation, Holden Knight Healthcare must be able to demonstrate for the specific purposes of processing personal information what that legal

---

[1] The right to data portability applies in the case of contract being the legal basis.

[2] The right to not being subject to automated decision-making, including profiling, does not apply where there is a necessity for the purposes and legal basis of a contract (or entering into a contract).

obligation is, third parties who receive the personal information under the auspices of the obligation, and any retention obligations required.

3.8 Vital Interests

When using vital interests, Holden Knight Healthcare must be able to demonstrate that there is a necessity to process personal information in the vital interests of the individual concerned.

3.9 Public Interest

When using public interest, Holden Knight Healthcare must be able to demonstrate that there is a need to store personal information in the interests of the public. For example, for public safety and security purposes, retaining staff information to pass to emergency services personnel given some event.

3. REQUIREMENTS

4.1 Notices

Individuals have the right to be informed regarding the specific purposes that their personal information is being processed before processing takes place, for how long the information will be stored and processed, who it is being shared with (including internationally), and if there is automated decision-making, including profiling.

4.2 Transfers

The DP Legislation prohibits us from transferring personal information to countries outside the European Economic Area (EEA), unless we first put in place additional safeguards. For example, before transferring information, we may need to enter into contracts with recipients in non-EEA countries which incorporate Standard Contractual Clauses approved by the EU Commission.

4.3 Any such transfers should be notified to the Data Protection Officer stating who the data is being shared with, and if it is subject to any automated decision-making, including profiling.

4.4 Retention

In accordance with the principle of Data Minimisation Holden Knight Healthcare will hold data for no longer than is necessary for the original purpose for which the data was collected. Holden Knight Healthcare has a duty to retain some staff and young person's personal data for a period of time following their departure from our care, mainly for legal reasons, but also for other purposes such as being able to provide references.

4.5 Different categories of data will be retained for different periods of time. Please see our data retention and Erasure Policy for more information.

4.6 Disposal of Information

Printed information will be shredded. Any computer or portable media containing information will be securely and permanently deleted and/or physically destroyed.

4.7 Data Protection by Design / Data Protection by Default - Approach

We must ensure that our policies reflect processes and a culture of respecting privacy. This includes ensuring that we are each accountable for the security and other safeguarding measures are adhered to, as well as collecting, processing storing, and only sharing it with those authorised and required to use it, only the personal information that is required, and only for as long as it is required for.

4.8 Data Protection Impact Assessment (DPIA)

DPIA guidance is to undertake an assessment from a risk-based perspective. Any new process or system that includes innovative technologies or processing personal information or monitoring individuals on a large scale, where there is a higher risk to rights and freedoms of individuals affected.

3. DATA SUBJECT RIGHTS

5.1 Summary of Rights

The subjects of personal information held by, or on behalf of, Holden Knight Healthcare ("Data Subjects") have a wide range of rights granted to them under the DP Legislation. Whilst we can make use of personal information for specific purposes and where we can lawfully justify such use, an individual can still exercise significant control over what we do. We need to operate our business and process personal information in a way which facilitates the rights of individuals to exercise this control.

5.2 Today's DP Legislation significantly enhances the rights available to individuals. A summary of each of the rights is set out below. It is important that requests from individuals wishing to exercise any of the rights below are quickly identified and sent to the appropriate person for preparing a response. Employees should not respond to such requests without first discussing the matter with your line manager, who may refer the matter to the Data Protection Officer.

5.3 Right to be informed

Individuals have the right to be informed of how their personal information is being processed. This must be provided in a privacy notice – the notice may be in the form of:

- a privacy statement or privacy policy, separate to a cookie policy (which is also required);
- an email signature, other correspondence, or information board in a public area;
- a privacy clause in an Employee Handbook; or
- a clause within the Terms and Conditions of a contract.

In general, individuals must be informed about:

- the purpose for processing their personal information,
- what information is processed, and
- for how long.

5.4 The notice should also include the contact details of Holden Knight Healthcare and our Data Protection Officer. Within the privacy notice, individuals also have the right to be informed whether any third parties are to be recipients of their personal information.

5.5 Similarly, in the same notice, individuals have the right to be informed whether their personal information will be transferred to 3rd countries or international organisations – generally outside the European Economic Area not covered by the 'adequacy' regime or other safeguards, such as Binding Corporate Rules or Standard Contract Clauses.

5.6 Right of access ('Subject Access Requests')

Individuals have the right to request that we:

(i) confirm, amongst other things, whether we are holding their personal information;
(ii) provide them with a copy of that information, and
(iii) provide them with supporting (and detailed) explanatory materials.

5.7 We must comply with Subject Access Requests without undue delay and at the latest within one month of the request (although this can be extended in limited circumstances), and we cannot charge individuals for making a request (except in specific situations).

5.8 Particular care should be taken if a request from one individual would result in personal information of another individual being disclosed [seek advice from the Data Protection Officer about whether such information should be redacted, or its disclosure justified]. Please contact the Data Protection Officer if you receive a request for the release of personal information.

5.9 Right to rectification

Individuals have the right to require us to rectify inaccuracies in personal data held about them. In some circumstances, if personal information records are incomplete or inconsistent, individuals have the right to require us to complete the data, make it consistent, or to record a supplementary statement correcting it. Advice should be sought from the Data Protection Officer if uncertain.

5.10 Right to erase ('the right to be forgotten')

Individuals have the right to have their personal information erased in certain specified situations – in essence where the continued processing of it does not comply with DP Legislation.

5.11 Where an individual makes an erasure request, we must respond without undue delay and in any event within one month (although this can be extended in limited circumstances). There are a number of exemptions which apply to such requests, and you should not assume that you should delete personal information simply because you have received a request of this nature. Such a request should be referred to the Data Protection Officer as soon as it is received.

5.12 Right to restriction

This right allows individuals, in certain situations, to restrict our use of their personal information. This might result in our use of it being limited to storage only which could mean we have to move personal information to separate IT systems, or temporarily block access to it.

5.13 This issue could arise in a situation where an individual is disputing the accuracy of information we hold, or where they are objecting to our right to continue to use their information and we need to take some time to establish whether we have a right to continue to do so. Such a request should be referred to the Data Protection Officer as soon as it is received.

5.14 Right to data portability

Data portability goes beyond rights of access and requires us to provide, on request, information to individuals in a structured, commonly used and machine-readable format. We could also be asked by an individual to transmit personal information directly to another data controller in the same format.

5.15 This right only applies to electronic records which have been provided to us by the individual themselves, or generated from their activity or are our observations of their activity (but not subsequent analysis of such activity), and only where we hold the personal information because we have the individual's consent or because we are fulfilling a contract with them.

5.16 Right to object

Individuals have an absolute right to object to their personal information being processed for the purpose of direct marketing. If we receive any such objection, we must immediately cease such marketing activities in respect of that individual.

5.17 Individuals have a wider right to object to processing we undertake which is justified on the basis that it is in our legitimate interests (rather than because we have their consent). If we receive an objection of this nature, we must assess the objection and carefully consider if we can demonstrate compelling legal grounds to continue to process the personal information.

5.18 Rights in relation to automated decision-making, including profiling

Individuals have rights which apply if we take decisions about them which are based solely on automated processing (i.e. without human intervention) and which produce significant or legal effects on the individuals.

5.19 Holden Knight Healthcare does not use automated decision making when processing personal data.

5.20 Right to complain

Individuals have the right to bring a complaint to the Information Commissioner, or other supervisory authority.

5.21 Right to bring legal proceedings

Individuals have the right to seek judicial remedy through the Courts.

5.22 Requests

Employees or other subjects of personal information held by, or on behalf of Holden Knight Care may exercise any of the rights specified above. These rights are subject to certain exemptions which are set out in the DP Legislation.

5.23 Any team member or other subject of personal information wishing to exercise any of these rights should make the request in writing to the Data Protection Officer. Holden Knight Healthcare aims to comply with any requests in relation to personal information as quickly as possible and in any event within the time specified by DP Legislation.

3. EMPLOYEE RESPONSIBILITIES

6.1 All Personnel are responsible for:

- checking any personal information which they provide to Holden Knight Healthcare is accurate and up to date;
- informing Holden Knight Healthcare of any changes to personal information which they have provided, for example change of address; and

- checking any information that Holden Knight Healthcare may send out from time to time, for example giving details of personal information that is held by Holden Knight Healthcare.

6.2 Responsibilities for other's data

If, as part of their responsibilities, staff have access to or use personal information about other people as part of their employment duties (for example, young person's, business point of contact or professional's personal information) they must comply with this policy and in Holden Knight Healthcare's other policies and procedures for processing personal information.

6.3 As an individual you are responsible for ensuring that:

- Any personal data that you hold is kept securely
- Personal information is not disclosed either orally or in writing, accidentally or otherwise to any unauthorised third party
- Personal information is not transferred internationally without checking first that the right safeguards are in place.
- You avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, it must be locked out of sight
- Passwords and logon information are not disclosed to anyone else
- Personal information is kept in a locked filing cabinet, or in a locked drawer, or
- If it is computerised, be password protected, or if kept temporarily on portable media be password protected and kept securely.
- If you are aware of a breach of security with passwords or logon information your line manager or the Data Protection Team are informed immediately

6.4 Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. In particular any **deliberate** or **serious** breach of this Data Protection Policy by a member of staff may lead to dismissal and even to criminal prosecution.

6.5 Access Restriction

Only those employees who strictly require access to personal information for their role should have such access, and all staff must make sure that personal information is not shared with anyone who do not need to see it.

6.6 Special Categories

Personal information about employees and others may include special categories of personal information or other information that needs to be treated sensitively. This is personal information relating to an individual'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;
- sexual life;

- biometric or genetic data (e.g. facial or iris imaging, or biological sample information.)
- commission or alleged commission of an offence;
- any proceedings for any offence or alleged offence, the disposal of such proceedings or any sentence imposed by a court

6.7 Particular care must be taken when dealing with any personal information falling under one or more of these headings. If in doubt, do take advice from the Data Protection Team or (if an employee related issue) the HR Team. In general, such personal information must be kept very secure and must only be allowed to be seen by a restricted number of people who need to know it. The Data Protection Officer will act as an intermediary between Holden Knight Healthcare, employees, suppliers, customers, partners and others.

3. EMAIL

7.1 Due to the ease with which large quantities of personal data can be accidentally or inappropriately exposed when using email staff should be particularly careful to use email in a considered manner. In particular:

- Email to addresses outside the "@holdenknight.com" domain should not include personal data beyond simple contact information (name, email, telephone, address, job title and place of work). If more extensive data needs to be provided an encrypted attachment can be used (MS Office encryption is adequate for low risk data) or a specialised secure transfer option may be used in high risk cases.
- If using an encrypted email attachment to send personal data do not include the password in the same email and preferably use a different communication method to send the password (e.g. SMS).
- Emails sent from "@holdenknight.com" addresses to "@holdenknight.com" addresses are restricted to the secure environment and may include personal data.
- Do not include any personal information in the "Subject" field of email regardless of the recipient, in particular do not include names or other potential identifiers.
- Staff should make it a habit to preferentially use "Bcc" rather than "Cc", "Cc" should only be used where it is necessary for all recipients to see replies.
- When using Distribution Lists to send emails to those outside Holden Knight Healthcare, ensure that email addresses are not shared. Use the "Bcc" facility so that email addresses are not displayed.

3. DBS CHECKS

8.1 Agreement to Holden Knight Healthcare processing certain types of personal data is a condition of employment for staff. This includes information about previous criminal convictions.

8.2 All members of staff and volunteers who come into contact with children will be subject to Enhanced DBS checks. Holden Knight Healthcare has a duty under the Children Act and other enactments to ensure that staff are suitable for the job. We also have a duty of care to all staff and volunteers, and must, therefore, make sure that employees and those who use Holden Knight Healthcare facilities do not pose a threat or danger to other users.

3. MEDICAL INFORMATION

9.1 Holden Knight Healthcare will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. We will only use the information in the protection of the health and safety of the individual.