Version 1.1
Last Updated: 10th November 2025

DATA PROTECTION POLICY

(FOR INTERNAL USE)

Sapphire Independent Housing Ltd

Contents

Introduction

1.1 Sapphire Independent Housing ("**Sapphire**") has a responsibility to ensure that it uses information about individuals in a way that is fair and justifiable. Information about individuals is referred to in this Policy as personal data.

1.2 Personal data is a wide concept. It includes any information that identifies an individual either directly (such as names and contact details) or indirectly (such as information which could be used to identify a person when linked to other information).

1.3 This Data Protection Policy (the "**Policy**") sets out how Sapphire handles the personal data of our customers, prospective customers, clients, suppliers, employees, workers and other third parties. It applies to all personal data we process, regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other data subject.

1.4 This Policy applies to all of Sapphire's staff, contractors and volunteers. You must read, understand and comply with this Policy when processing personal data on Sapphire's behalf. Data protection is the responsibility of everyone within Sapphire. This Policy sets out what we expect from you when handling personal data to enable Sapphire to comply with applicable law. Your compliance with this Policy is mandatory.

1.5 This Policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from Heather Thomas, CEO.

1.6 There is a Privacy Notice relating to people using our website at www.sih.org. There is a Privacy Notice that describes the way in which Sapphire processes your personal data as an employee or a contractor at the Staff Room.

1.7 Should you have any questions about this Policy, please get in touch with HR or Heather Thomas, CEO.

1.8 This Policy may be amended at any time. You will be notified of any significant changes.

Respecting people's right to privacy and protecting their personal data is the responsibility of all of us. It is part of being an ethical business. This Policy will help us to comply with the law and to ensure that our business practices reflect our values as a company.

2. Background

2.1 What is data protection law?

Data protection law gives people the right to control how their **personal data** is used. It is a detailed "working out" of Article 8 of the European Convention on Human Rights – the right to a private and family life. Data protection law places obligations on organisations that use personal data. It ensures that people's data is used ethically and fairly and that any interference with the right to privacy is lawful, proportionate and justifiable. The UK data protection regime consists of the UK GDPR and the Data Protection Act 2018.

2.2 What are the consequences if we get it wrong?

Getting it wrong can be serious. Breaches of data protection law could lead to complaints from individuals, compensation claims and even investigations or fines by regulators. The regulator in the UK is the Information Commissioner's Office (**ICO**).

Breaches of data protection law can also damage the reputation of Sapphire and the relationship of trust between us and the people whose data we process.

The Data Protection Principles

3. Transparency

We must be transparent about the personal data that we hold, including describing the purposes for which we use personal data

3.1 Understanding the principle

Being open and transparent in the way we use and share personal data is important. Data protection law requires us to provide information to individuals about how we use their personal data. The law sets out exactly what information must be provided. Sapphire has drafted privacy notices (also known as privacy policies) that comply with these requirements.

3.2 What this means in practice

3.2.1 At the time we collect individuals' personal data, we need to provide them with information including:

(a) The purposes of the processing;

(b) The lawful basis for the processing;

(c) The legitimate interests for the processing (if applicable);

(d) The categories of personal data obtained (if the personal data is not obtained from the individual it relates to);

(e) The recipients or categories of recipients of the personal data;

(f) The details of transfers of the personal data to any third countries or international organisations (if applicable).

3.2.2 We have a general privacy notice on our website that sets out the relevant information that we need to give to individuals to comply with transparency requirements when they engage with us. Where we undertake specific processing, we may provide additional privacy notices as required.

3.2.3 If we obtain personal data from a source other than the individual it relates to, we must provide the individual with the information set out at 3.2.1 above within a reasonable period of obtaining the personal data and no later than one month after receiving it.

3.2.4 If we intend to communicate with an individual, we must provide them with our privacy notice when the first communication takes place.

3.2.5 Where we plan to disclose the data to someone else, we must provide the individuals who the data relates to with the information set out above at 3.2.1. We must do this at the latest at the point at which the data is first disclosed.

3.2.6 Privacy notices should be regularly reviewed and updated. If we plan to use personal data for a new purpose, we must update our privacy notice and communicate the changes to individuals before starting the new processing.

4. Lawful basis

We must have a lawful basis for collecting and using personal data

4.1 Understanding the principle

4.1.1 Under data protection law, the processing of personal data must be lawful. This requirement has two elements:

(a) First, we must be able to identify that at least one of the legal bases set out in the UK GDPR applies; and

(b) Second, the collection and use must be generally lawful (so for example it must not breach confidentiality).

4.1.2 Where the personal data is sensitive, further requirements apply which must be satisfied before it can be used.

4.2 Legal bases

4.2.1 There are six legal bases. Examples of the legal bases which Sapphire normally relies on are:

4.2.2 **Legitimate interests**: this legal basis can be relied on where (i) Sapphire has a good reason to collect and use personal data (for example where we are processing information to allow us to ensure that our website functions correctly); and (ii) where those good reasons are not outweighed by any prejudice to individuals' privacy rights.

4.2.3 **Contract**: where Sapphire needs to process the personal data to carry out its obligations under a contract with the individual, or because the individual has asked us to take specific steps before entering into a contract. This means that the contract legal basis is relatively narrow. It doesn't apply where two organisations are contracting. In such cases, the legitimate interests legal basis is likely to be the most appropriate legal basis to rely on for the processing of personal data under the contract.

4.2.4 **Consent**: where the individual has given clear consent to the processing of their personal data. Note that individuals can withdraw the consent that they provide to us at any time. Where consent is withdrawn the processing must stop, unless there is a very good reason to retain the personal data. One example might be where you need to keep a record of the withdrawal of consent, for example to maintain suppression records so that we can comply with direct marketing rules. The individual's ability to withdraw consent might mean that it is not always the most practical legal basis. You should try to avoid consent if another legal

basis is available. If you need advice on this issue, you should contact HR or Heather Thomas, CEO.

4.3 In terms of the requirement that the processing of personal data is generally lawful, an example might be where personal data is provided on a confidential basis, such as information relating to an individual's health or the health of a family member. If disclosing that information amounted to a breach of confidentiality, then the disclosure would also be unlawful under data protection law.

4.4 **What this means in practice**

Sapphire has reviewed its collection and use of personal data to ensure that it complies with these requirements. However, where we are changing our processes or implementing new technology or services, we must ensure that data protection compliance has been considered. Please contact Heather Thomas if you are considering implementing changes, to ensure that our obligations to process data lawfully are met.

5. Fairness

We must process personal data in a way that is fair to individuals

5.1 **Understanding the principle**

The processing of personal data must be fair. This means that we must treat people in an ethical way when it comes to processing their personal data. We must not interfere with their privacy rights in a manner that cannot be justified.

5.2 **What this means in practice**

5.2.1 We need to consider how the processing may affect individuals and be able to justify any adverse impact.

5.2.2 We should only process personal data in a way that people would expect or be able to justify any unexpected processing.

5.2.3 We must not deceive or mislead people when we collect their personal data.

6. Purpose limitation

We must collect personal data for a specified, explicit and legitimate purpose and not further process the data in a way that is incompatible with that purpose.

6.1 **Understanding the principle**

We must be clear about our purposes for processing the personal data and make appropriate records. Our purposes must be reflected in our privacy notice. We can only use the personal data for a new purpose if either this is compatible with our original purpose, where we get consent from individuals or where we are processing the personal data on the basis of a clear obligation or function set out in law.

6.1.1 For example, if we collect personal data such as a contact number or email address in order to update a person about our activities, we should not then use it for a different purpose such as sharing it with other organisations for marketing purposes.

6.2 **What this means in practice**

We must:

(a) clearly identify our purpose or purposes for processing;

(b) record those purposes;

(c) include details of our purposes in our privacy notices;

(d) regularly review our processing and update our documentation and our privacy notice where required;

(e) check that any new use of personal data is compatible with our original purpose. If not, we need to get specific consent for the new purpose, unless we are processing on the basis of an obligation or function set out in law.

7. Accuracy

We must keep personal data accurate and (where necessary) up to date

7.1 **Understanding the principle**

Processing inaccurate information can be detrimental to individuals and to Sapphire. The main way of ensuring that personal data is kept accurate and up to date is by checking that the sources we use to obtain personal data are reliable. Individuals should be actively encouraged to inform us when their personal data changes. Note however that what is accurate can be a matter of opinion. Individuals are not entitled to use the accuracy principle to impose their view of the facts.

7.2 **What this means in practice**

(a) Aim to collect personal data directly from individuals where reasonable or possible;

(b) Ask individuals to update or confirm their personal data;

(c) We should take every reasonable step to erase or rectify inaccurate personal data;

(d) Where accuracy is a matter of opinion and you decide not to change the record when requested by an individual, make sure that you have noted your reasons for not amending the relevant information;

(e) Note that it may not be necessary to update personal data in all circumstances, for example where you are keeping it in order to have a record which relates to a past event.

8. Data retention

We must keep personal data only for as long as is necessary for a specific purpose and delete personal data we no longer need

8.1 Understanding the principle

(a) We should not keep personal data for longer than we need it. Where it is no longer needed it should be deleted.

(b) Note that laws or contractual obligations may require that certain personal data be retained for a specified length of time. It may also be prudent to keep certain personal data for a specific period so that we are able to properly defend any legal claims or manage an ongoing business relationship (for example, the typical limitation period for claims in the UK is 6 years).

8.2 What it means in practice

We must follow all internal data retention policies in relation to:

(a) The key applicable retention requirements from both a business and (where applicable) legal perspective.

(b) Procedures for ensuring that personal data is properly retained and securely destroyed.

(c) The process for suspending the destruction of documents in situations relating to pending, threatened or reasonably likely litigation, or regulatory investigations.

8.3 See **Annex A** for Sapphire's data retention policy and retention schedule.

9. Data minimisation

We must not collect more personal data than we need for our purposes

9.1 Understanding the principle

We must be clear about why we need to collect the personal data. This is even more important where the data is sensitive. We must not collect personal data on the basis that it might be useful in the future if it does not fulfil a current or foreseeable purpose.

9.2 What it means in practice

9.2.1 We should only collect personal data we need for our specified purposes.

9.2.2 We should have sufficient personal data to properly fulfil those purposes.

9.2.3 We should review the data we hold at regular intervals and delete anything we don't need.

10. Taking appropriate security measures

We must always take appropriate steps to protect personal data

10.1 Understanding the principle

10.1.1 Personal data must be kept secure. We have technical controls and security measures, as well as policies and procedures to protect personal data from unauthorised access, disclosure, loss, destruction or damage.

10.1.2 Where we fail to take appropriate security measures, we may suffer a personal data breach (i.e. a breach of security that leads to the unauthorised access, use or disclosure of personal data). We may be required to notify the relevant regulator and possibly also the individuals affected. If we fail to take steps to keep data secure, we could cause real harm to those individuals whose personal data has been compromised. Examples of potential harms include identity fraud or greater exposure to scams and financial loss. Individuals could also suffer discrimination or other harm or reputational damage if sensitive information about them is made public. Loss or compromise of the personal data we hold can also inflict reputational damage and leave us at risk of regulatory action.

10.2 What it means in practice

We must comply with the appropriate procedures set out in our information security policy. This means that we:

(a) analyse the risks in relation to our processing and use this analysis to assess the appropriate level of security required. The level of security needed will depend on the nature of the data. The more sensitive and confidential the data, the more stringent the security measures should be;

(b) take account of the state of the art and costs of implementation when deciding what measures to put in place;

(c) follow and regularly review our IT and security policies, putting in place new or updated measures where necessary;

(d) use encryption and/or pseudonymisation where it is appropriate to do so;

(e) understand the requirements of confidentiality, integrity and availability for the personal data we process;

(f) ensure we can restore access to personal data in the event of any incidents, such as by putting in place an appropriate backup process;

(g) ensure that our data processors also implement appropriate technical and organisational measures.

10.3 Do you suspect a personal data breach has taken place?

10.3.1 If we experience a personal data breach, we will take measures to mitigate possible adverse effects. It is imperative that we act quickly if we suspect a personal data breach in order to protect individuals and Sapphire. Where personal data breaches reach a certain threshold of severity, we need to notify the relevant regulator of what has happened within 72 hours of Sapphire becoming aware of a breach. Timeframes are therefore extremely tight.

10.3.2 If you become suspicious or are aware of any breach, you must comply with the steps set out in our information security policy and immediately contact HR or Heather Thomas, CEO.

11. Accountability

We must comply with the UK GDPR and be able to demonstrate our compliance

11.1 Understanding the principle

We must take responsibility for complying with the UK GDPR and be able to demonstrate our compliance.

11.2 What it means in practice

(a) Everyone at Sapphire should take responsibility for complying with the UK GDPR;

(b) We must keep evidence of the steps we take to comply with the UK GDPR;

(c) We must have appropriate technical and organisational measures in place, such as:

(i) adopting and implementing data protection policies (where proportionate);

(ii) putting appropriate data protection measures in place throughout the lifecycle of our processing operations;

(iii) putting written contracts in place with organisations that process personal data on our behalf;

(iv) maintaining documentation of our processing activities;

(v) implementing appropriate security measures;

(vi) recording and, where necessary, reporting personal data breaches;

(vii) carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;

(viii) appointing a data protection officer (where necessary); and

(ix) reviewing and updating our accountability measures at appropriate intervals.

12. Data subject rights requests

We should know how to recognise a data subject rights request and what

procedures must be followed when we receive one

12.1 The UK GDPR provides the following rights for individuals:

(a) The right to be informed;

(b) The right of access;

(c) The right to rectification;

(d) The right to erasure;

(e) The right to restrict processing;

(f) The right to data portability;

(g) The right to object;

(h) Rights in relation to automated decision making and profiling.

Note that none of these rights are absolute – just because an individual has raised these rights does not mean that Sapphire must comply with them. They are subject to numerous qualifications and exemptions. Responding to them is therefore a complex matter. You should notify HR or Heather Thomas, CEO, as soon as possible if you receive a notification from an individual that they wish to exercise one of these rights. Timeframes are short, so requests to exercise these rights need to be acted upon quickly.

13. The right to be informed

The right to be informed is explained further above at section 3 – transparency.

14. The right of access

(a) Individuals have the right to request their personal data and (subject to any applicable exemptions) to receive a copy of that data and other supplementary information;

(b) A request for personal data is also known as a data subject access request ("**DSAR**");

(c) A valid request can be made verbally or in writing including through social media;

(d) A DSAR does not have to mention the UK GDPR – it is enough that an individual asks for information about themselves – this triggers the right;

(e) A DSAR must be dealt with quickly – usually within one month of receipt of the request, so you need to action it immediately. The timetable is very tight, particularly if there is a lot of data to collect and consider.

15. Right to rectification

(a) Individuals have the right to have inaccurate personal data corrected or completed if it is incomplete;

(b) A request can be made orally or in writing;

(c) Requests must be responded to within one month of receipt;

(d) The UK GDPR does not need to be mentioned in order for the right to be engaged;

(e) Exemptions or qualifications may apply.

16. Right to erasure

(a) The UK GDPR provides a right for individuals to have personal data erased;

(b) The right to erasure is also known as 'the right to be forgotten';

(c) The right only applies in certain circumstances;

(d) Individuals can make a request for erasure verbally or in writing and do not need to mention the UK GDPR in order for the right to be engaged;

(e) We have one month to respond to a request.

17. Right to restrict processing

(a) Individuals have the right to request the restriction or suppression of their personal data;

(b) This right only applies in certain circumstances;

(c) When processing is restricted, we are permitted to store the personal data, but not use it.

(d) An individual can make a request for restriction verbally or in writing and does not need to mention the UK GDPR in order for the right to be engaged;

(e) We have one calendar month to respond to a request.

(f) This right has close links to the right to rectification (see section 15) and the right to object (see section 19).

18. Right to data portability

(a) The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services;

(b) It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

19. Right to object

(a) The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances;

(b) Individuals have an absolute right to stop their data being used for direct marketing;

(c) In other cases where the right to object applies we may be able to continue processing if we can show that we have a compelling reason for doing so;

(d) An individual can make an objection verbally or in writing and does not need to mention the UK GDPR in order for the right to be engaged;

(e) We have one calendar month to respond to an objection.

20. Rights related to automated decision-making including profiling

(a) The UK GDPR confers rights on individuals in relation to:

(i) automated individual decision-making (making a decision solely by automated means without any human involvement); and

(ii) profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

(b) The UK GDPR contains additional rules to protect individuals if an organisation carries out solely automated decision-making that has legal or similarly significant effects on them.

21. Using a processor to process personal data on our behalf

We must ensure that a contract is in place between Sapphire and its processors which contains appropriate terms. Prior to appointment we should ensure that our processors have implemented appropriate technical and organisational measures, to ensure a level of security appropriate to the risk posed by the processing.

21.1 Understanding the concept

Where a processor processes personal data on Sapphire's behalf (for example, as a website host or where providing a customer relationship management system etc.) we must enter into prescribed contractual terms. We must also ensure that the processor has appropriate measures in place to protect the data.

21.2 What it means in practice

21.2.1 Before we engage a supplier, we must carry out appropriate and proportionate due diligence which considers the supplier's security measures for processing personal data and the location where they will be processing personal data. Examples of the sorts of things that we should check are:

(a) the extent to which their processing complies with industry standards, if these apply in the context of the processing;

(b) whether they have sufficient technical expertise to assist Sapphire, e.g. in carrying out obligations under Articles 32 – 36 of the UK GDPR (technical measures, breach notifications and data protection impact assessments);

(c) whether they have relevant documentation, e.g. privacy policy, record management policy and information security policy.

21.2.2 We must enter into a written contract with our processor. The provisions must address certain matters including:

(a) the subject matter and duration of the processing;

(b) the nature and purpose of the processing;

(c) the type of personal data and categories of data subject;

(d) use of appropriate security measures;

(e) audits and inspections.

22. Data sharing with other controllers

We must only disclose personal data to other controllers (e.g. organisations which are our partners) where we have appropriate agreements in place

22.1 Understanding the concept

At times, we may disclose personal data to other controllers, for example where we are contracting with them. The contract will need to contain clauses about the sharing of personal data. The ICO's data sharing code of practice sets out in more detail what is required.

22.2 What this means in practice

The clauses will need to address matters such as:

(a) The fact that both parties are controllers of the personal data;

(b) That they should cooperate in relation to requests they receive from data subjects wanting to exercise their rights (for example the right of subject access);

(c) That they will cooperate in the event of a personal data breach.

If a project you are working on involves the sharing of personal data with another controller, you should contact HR who will be able to assist.

23. Complying with the requirements relating to international data transfers

International transfers of personal data are subject to certain legal restrictions and therefore we must ensure that all transfers are subject to appropriate safeguards through putting contracts in place

23.1 Understanding the rules

Data protection law restricts international transfers of personal data. There must be a mechanism in place, which ensures that personal data transferred abroad is protected to the

same standard as personal data processed within the UK. In broad terms, there are three mechanisms which enable international transfers of personal data: adequacy decisions, standard data protection clauses and (as a last resort) derogations.

23.2 Adequacy decisions

An adequacy decision is a decision (by the Secretary of State in the UK) that the protection of personal data in the country to which the data is being sent is not materially lower than that in the UK, in which case no further steps are required to transfer personal data to that country. The UK maintains a list of countries which provide adequate protection for personal data, which can be found here.

23.3 Standard data protection clauses

If there is no applicable adequacy decision, then we need to consider other methods to protect the data when it is transferred abroad. The most frequently used method of transferring personal data to third countries which are not subject to an adequacy decision is a set of 'standard contractual clauses' that have been approved for international data transfers by the ICO. These provisions have been included in a document known as the International Data Transfer Agreement (**IDTA**). This is a complex area so please consult HR if you are considering transferring personal data abroad.

We are also required to carry out 'transfer risk assessments' in respect of any international transfer of personal data to countries that are not adequate. The transfer risk assessment requires us as the transferor to take into account the data protection law and practices of the countries to which the data will be sent, including the ability of public authorities in those countries to access personal data. Depending on the results of this assessment, we may need to implement further measures to ensure that the personal data is adequately protected after it is transferred. The ICO has issued a transfer risk assessment tool here for use in the UK. Please consult HR to review and approve any transfer risk assessment.

23.4 Derogations

In exceptional circumstances and taking a risk-based approach, we may rely on derogations or exceptions to transfer personal data to a third country. Contact HR before deciding to rely on a derogation to transfer personal data overseas.

23.5 What it means in practice

In order to comply with this principle, we must not transfer any personal data to a third country without checking what mechanism is being relied upon to do so (either adequacy, the IDTA or a derogation).

24. Special Category Personal Data

We must ensure that we only collect special categories of data if it is necessary for us to do so. Special category personal data requires a higher level of protection, due to its sensitivity.

24.1 Understanding the concept

This type of data is information revealing an individual's **racial or ethnic origin**, **political opinions**, **religious or other beliefs**, **trade union membership**, **genetic data** or **biometric data** (for the purpose of uniquely identifying an individual), **health** and **sex life** or **sexual orientation**. It requires additional safeguards and restrictions on its use.

24.2 **What this means in practice**

We must always assess whether processing of the special category data is necessary for the purpose we have identified. We must be satisfied there is no other reasonable and less intrusive way to achieve that purpose;

(a) We must identify an Article 6 UK GDPR lawful basis for processing the special category data;

(b) We must identify an appropriate Article 9 UK GDPR condition for processing the special category data;

(i) Where required, we must also have identified an appropriate condition for the processing of the data under Schedule 1 to the Data Protection Act 2018;

(ii) We must have documented which special categories of data we are processing;

(iii) Where required, we have an appropriate policy document in place;

(iv) We should have considered whether we need to complete a Data Protection Impact Assessment ("DPIA");

(v) We should include specific information about our processing of special category data in our privacy information for individuals;

(vi) If we use special category data for automated decision-making (including profiling), we must check that we comply with the relevant provisions;

(vii) We should consider whether the risks associated with our use of special category data affect our other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs);

(c) You must always inform HR of any planned significant use of special categories of data, so that they can verify the legitimacy of such use.

25. New or high-risk projects

Where we are undertaking new projects or developing our processes and systems we must consider whether we need to carry out a Data Protection Impact Assessment. Data protection compliance must be built into the design of our systems.

25.1.1 **Understanding the rules**

We must:

(a) carry out a Data Protection Impact Assessment (**DPIA**) where the collection and use of personal data is likely to result in a high risk to the rights and freedoms of individuals.

(b) adopt privacy by design and privacy by default in all systems, databases, tools and features we build to collect and use personal data.

25.1.2 **What this means in practice**

We must:

(a) consider carrying out a DPIA in any significant project involving the use of personal data.

(b) consider whether to complete a DPIA involving the following:

(i) evaluation or scoring;

(ii) automated decision-making with significant effects;

(iii) systematic monitoring;

(iv) processing of sensitive data or data of a highly personal nature;

(v) processing on a large scale;

(vi) processing of personal data concerning vulnerable data subjects;

(vii) innovative technological or organisational solutions;

(viii) processing that involves preventing data subjects from exercising a right or using a service or contract.

We must always carry out a DPIA if we plan to:

(a) use systematic and extensive profiling or automated decision-making to make significant decisions about people;

(b) process special category data or criminal offence data on a large scale;

(c) systematically monitor a publicly accessible place on a large scale;

(d) use innovative technology in combination with any of the criteria in the European Data Protection Board's guidelines;

(e) use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

(f) carry out profiling on a large scale;

(g) process biometric or genetic data in combination with any of the criteria in the European Data Protection Board's guidelines;

(h) combine, compare or match data from multiple sources;

(i) process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European Data Protection Board's guidelines;

(j) process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European Data Protection Board's guidelines;

(k) process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

(l) process personal data that could result in a risk of physical harm in the event of a security breach.

We must carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

If we decide not to carry out a DPIA, we document our reasons.

25.1.3 Data protection by design and by default:

(a) We must ensure that any privacy settings are by default set to the most privacy protective setting.

(b) We must consider data protection issues as part of the design and implementation of systems, services, products and business practices.

(c) We must make data protection an essential component of the core functionality of our processing systems and services.

(d) We should anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

(e) We should only process the personal data that we need for our purpose(s), and ensure that we only use the data for those purposes.

(f) We must ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

(g) We must provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

(h) We should adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.

(i) We must provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

(j) We must offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

(k) We must only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

(l) When we use other systems, services or products in our processing activities, we should make sure that we only use those whose designers and manufacturers take data protection issues into account.

(m) We should use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

26. Complying with this Policy

26.1 What happens if we don't comply with this Policy?

Anyone who perceives that this Policy has not been complied with (even inadvertently) must immediately inform HR or Heather Thomas, CEO. Alerting us early to an actual or perceived breach is the best way of preventing negative outcomes. Deliberate or significant breaches/attempts to cover up breaches of the Policy are serious matters and could lead to disciplinary action or dismissal.

26.2 Are there exceptions to compliance with data protection law?

In broad terms, data protection law should not stand in the way of organisations doing sensible things with personal data. Therefore, if the framework appears to present a barrier to justifiable and appropriate business practices it may be that you have not understood the rules properly or there may be a relevant exemption from the rules which applies in your circumstances. If you consider that data protection rules are presenting an arbitrary or disproportionate barrier to being able to properly carry out your functions, then it may be that the position needs to be considered in more detail. In those circumstances, please contact HR.

27. Training

We require all relevant employees and contractors to receive training on data protection, both when they take up their role and at regular intervals throughout their time at Sapphire.

28. Implementation

This Policy is effective from 03/12/2025.

29. Updates and contact

Updating this Policy is the responsibility of Head of HR & Central Services. Queries and feedback should be directed to Beverly Finn. Date of last review: 10/11/2025