Volunteer Cornwall
Data Sharing Code of Practice

Introduction

Under the right circumstances and for the right reasons, data sharing across Volunteer Cornwall and between organisations can play a crucial role in providing a better, more efficient service to our clients.

It is important however that client's rights under the General Data Protection Regulation (GDPR) are respected and staff that don't understand what can and cannot be done legally are as likely to disadvantage their clients through excessive caution as they are by carelessness. Clients must be able to benefit from the responsible sharing of information, confident that their personal data is being handled responsibly and securely.

This code of practice is inevitably written in general terms, providing a framework for Volunteer Cornwall to make good quality decisions about data sharing. The code cannot provide detailed advice relevant to every situation in which data sharing takes place. As the name suggests, this code is about 'practice' – about doing, about delivering information rights in the real world. Adopting its good practice recommendations will help Volunteer Cornwall to make the best use of the data it holds to deliver the highest quality of service, whilst avoiding the creation of the opaque, excessive, and insecure information systems that can generate so much public distrust.

About the code

This code explains how the General Data Protection Regulation (GDPR) applies to the sharing of personal data. It also provides good practice advice that will be relevant to all staff who share personal data.

Who should use this code of practice?

Any member of staff or volunteer who is involved in the sharing of personal data should use this code to help them to understand how to adopt good practice.

How the code can help

Adopting the good practice recommendations in this code will help you to collect and share personal data in a way that is fair, transparent and in line with the rights and expectations of the people whose information you are sharing. The code will help you to identify the issues you need to consider when deciding whether to share personal data. It should give you confidence to share personal data when it is appropriate to do so and should also give you a clearer idea of when it is not acceptable to share data.
Specific benefits of this code include:

- minimise risk of breaking the law and consequent enforcement action.
- better public trust by ensuring that legally required safeguards are in place and complied with
- better protection for individuals when their data is shared.
- increased data sharing when this is necessary and beneficial.
- greater trust and a better relationship with the people whose information you want to share.
- reduced reputational risk caused by the inappropriate or insecure sharing of personal data.
- a better understanding of when, or whether, it is acceptable to share information without people's knowledge or consent or in the face of objection; and
- reduced risk of questions, complaints, and disputes about the way you share personal data.

What do we mean by 'data sharing'?

By 'data sharing' we mean the disclosure of data from Volunteer Cornwall to a third-party organisation or organisations, or the sharing of data between different parts of Volunteer Cornwall. Data sharing can take the form of:

- a reciprocal exchange of data.
- providing data to a third party or parties.
- several organisations pooling information and making it available to each other.
- several organisations pooling information and making it available to a third party or parties.
- exceptional, one-off disclosures of data in unexpected situations; or
- different parts of Volunteer Cornwall making data available to each other.

Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared. Neither the GDPR, nor this code of practice, apply to that type of sharing.

The code covers the two main types of data sharing:

- systematic, routine data sharing where the same data sets are shared within Volunteer Cornwall for an established purpose.
- exceptional, one-off decisions to share data for any of a range of purposes.

Different approaches apply to these two types of data sharing and the code of practice reflects this. Some of the good practice recommendations that are relevant to systematic, routine data sharing are not applicable to one-off decisions about sharing.

'Systematic' data sharing

This will generally involve routine sharing of data sets between organisations for an agreed purpose. It could also involve a group of organisations arranging to 'pool' their data for specific purposes.

Ad hoc or 'one-off' data sharing

Much data sharing takes place in a pre-planned and routine way. However, Volunteer Cornwall may also decide, or be asked, to share data in situations which are not covered by any routine agreement. In some situations, this may involve a decision about sharing being made urgently.

Sharing within Volunteer Cornwall

When we talk about 'data sharing' most people will understand this as sharing data between organisations. However, the data protection principles also apply to the sharing of information within an organisation – for example between the different departments of Volunteer Cornwall. Whilst not all the advice in this code applies to sharing within Volunteer Cornwall, much of it will, especially as the different parts of the organization can have very different approaches to data protection, depending on their functions.

Data sharing and the law

Before sharing any personal data, you hold, you will need to consider all the legal implications of doing so. Your ability to share information is subject to several legal constraints which go beyond the requirements of the GDPR. There may well be other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence that may affect your ability to share personal data. A duty of confidence may be stated, or it may be implied by the content of the information or because it was collected in circumstances where confidentiality is expected – medical or banking information, for example.

If you wish to share information with another person, whether by way of a one-off disclosure or as part of a large-scale data sharing arrangement, you need to consider whether you have the legal power or ability to do so. This is likely to depend, in part, on the nature of the information in question – for example whether it is sensitive personal data.

The legal framework that applies to private and third sector organisations differs from that which applies to public sector organisations, which may only act within their statutory powers. However, all bodies must comply fully with the data protection principles.

Most voluntary organisations have a general ability to share information provided this does not breach the Data Protection Act or any other law. It is advisable to check the memorandum and articles of association, to make sure there are no restrictions that would prevent Volunteer Cornwall sharing personal data in a particular context.

Voluntary sector organisations should have regard to any specific regulation or guidance about handling individuals' information as this may affect Volunteer Cornwall's ability to share information. We should also be aware of the legal issues that can arise when sharing personal data with public sector bodies. This becomes more of an issue as the voluntary sector is carrying out a wider range of traditionally public sector functions.

Deciding to share personal data.

Factors to consider.

When deciding whether to enter an arrangement to share personal data (either as a provider, a recipient or both) you need to identify the objective that it is meant to achieve. You should consider the potential benefits and risks, either to individuals or society, of sharing the data. You should also assess the likely results of not sharing the data. You should ask yourself:

- **What is the sharing meant to achieve?**

You should have a clear objective or set of objectives. Being clear about this will allow you to work out what data you need to share and who with. It is good practice to document this.

- **What information needs to be shared?**

You shouldn't share all the personal data you hold about someone if only certain data items are needed to achieve your objectives. For example, you might need to share somebody's current name and address but not other information you hold about them.

- **Who requires access to the shared personal data?**

You should employ 'need to know' principles, meaning that other organisations should only have access to your data if they need it, and that only relevant staff within those organisations should have access to the data. This should also address any necessary restrictions on onward sharing of data with third parties.

- **When should it be shared?**

Again, it is good practice to document this, for example setting out whether the sharing should be an on-going, routine process or whether it should only take place in response to events.

- **How should it be shared?**

This involves addressing the security surrounding the transmission or accessing of the data and establishing common rules for its security.

- **How can we check the sharing is achieving its objectives?**

You will need to judge whether it is still appropriate and confirm that the safeguards still match the risks.

- **What risk does the data sharing pose?**

For example, is any individual likely to be damaged by it? Is any individual likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

- **Could the objective be achieved without sharing the data or by anonymizing it?**

It is not appropriate to use personal data to plan service provision, for example, where this could be done with information that does not amount to personal data.

- **Do I need to update my notification?**

You need to ensure that the sharing is covered in your ICO register entry.

- **Will any of the data be transferred outside of the European Economic Area (EEA)?**

If so, you need to consider the requirements of the GDPR.

Conditions for processing

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

For processing to be lawful under the GDPR, organisations need to identify a lawful basis before they can process personal data. These were referred to "conditions for processing" under the Data Protection Act. It is important that the lawful basis for processing personal data is determined and documented.

Organisations processing sensitive personal data, for example information about a person's health, will need to satisfy a further, more exacting condition. It is important to be clear that meeting a condition for processing will not in itself ensure that the sharing of personal data is fair or lawful. These issues need to be considered separately.

Consent

Consent under GDPR must be a freely given, specific, informed, and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes, or inactivity. Consent must also be separate from other terms and conditions, and there must be simple ways for people to withdraw consent.

Consent must be verifiable, and individuals generally have more rights where you rely on consent to process their data.

There are other lawful bases apart from consent, for example, where processing is necessary for the purposes of Volunteer Cornwall's legitimate interests.

Consent or explicit consent for data sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so.
- the individual would be likely to object should the data be shared without his or her consent; or
- the sharing is likely to have a significant impact on an individual or group of individuals.

Under GDPR it is not necessary to refresh all existing DPA consents, but they must meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn.

Fairness and transparency

The GDPR requires that personal data be processed fairly and in a transparent manner. This means that people should generally be aware of which organisations are sharing their personal data and what it is being used for.

In a broader sense, fairness also requires that where personal data is shared, this happens in a way that is reasonable, and that people would be likely to expect and would not reasonably object to if given the chance. You need to think about this before you first share any personal data. This applies equally to routine data sharing or a single, one-off disclosure.

The right to be informed/Privacy notices.

The right to be informed encompasses Volunteer Cornwall's obligation to provide "fair processing information", typically through a privacy notice. The GDPR emphasizes the need for transparency over how personal data is used.

Much of the guidance on privacy notices is particularly relevant in data sharing contexts because of the need to ensure that people know who is sharing their personal data and what it is being used for.

In a data sharing context, a privacy notice must be:

- concise, transparent, intelligible, and easily accessible.
- written in clear and plain language, and
- free of charge.

You should provide a privacy notice at the time the data is collected. If you have already collected their personal data, then you need to provide them with the information as soon as you decide that you're going to share their data or as soon as possible afterwards.

In some cases, a single privacy notice may be enough to inform the public of all the data sharing that you carry out. However, if you are engaged in various significant data sharing activities, it is good practice to provide information about each one separately. This will allow you to give much more tailored information, and to target it at the individuals affected by the sharing. There is a danger that individuals affected by data sharing will not be able to find the information they need if we only publish one all-encompassing privacy notice.

It is good practice to review the privacy notice regularly so that it continues to reflect accurately the data sharing you are involved in. Any significant changes to your privacy notice need to be publicized appropriately – depending primarily on the impact of the changes on individuals.

What should you tell the individual?

Data sharing typically involves personal data being disclosed between several organisations, all of whom have a responsibility to comply with the GDPR.

The information that should be supplied to individuals is as follows:

- Identity and contact details of the data controller.
- Purpose of the processing and the lawful basis for the processing.
- The legitimate interest of the controller is applicable.
- Categories of personal data.
- Any recipients or categories of recipients of the personal data.
- Details of transfers to outside countries if applicable.
- Retention period or criteria for determining the retention period.
- The existence of each data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint.

- The source the personal data originates from and whether it came from publicly accessible sources.
- Whether the provision of personal data was part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.
- The existence of automated decision making and information about how decisions are made.

Sharing without the individual's knowledge

The GDPR rules that individuals should be aware that personal data about them has been, or is going to be, shared.

You can share without an individual's knowledge in cases where, for example, personal data is processed for:

- the prevention or detection of crime.
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty.

Security

The GDPR requires Volunteer Cornwall to have appropriate technical and organisational measures in place when sharing personal data. We may be familiar with protecting information we hold ourselves but establishing appropriate security in respect of shared information may present new challenges.

It is good practice to take the following measures in respect of information that you share with other organisations, or that other organisations share with you.

- Review what personal data we receive from other organisations, making sure we know its origin and whether any conditions are attached to its use.
- Review what personal data we share with other organisations, making sure we know who has access to it and what it will be used for.
- Assess whether we share any data that is particularly sensitive. Make sure we afford this data a suitably high level of security.
- Identify who has access to information that other organisations have shared. with us, 'need to know' principles should be adopted. You should avoid giving all your staff access to shared information if only a few of them need it to carry out their job.
- Consider the effect a security breach could have on individuals.
- Consider the effect a security breach could have on Volunteer Cornwall in terms of cost, reputational damage, or lack of trust from our customers or clients.

This can be particularly acute where an individual provides their data to an organisation, but a third-party recipient organisation then loses the data.

- We should aim to build a culture within Volunteer Cornwall where employees know and understand good practice, in respect of 'its own' data and that received from another organisation. Staff should be aware of security policies and procedures and be trained in their application. We will need to:
- design and organise our security to fit the type of personal data we disclose or receive and the harm that may result from a security breach.
- be clear about which staff members in the organisations involved in the sharing are responsible for ensuring information security. They should meet regularly to ensure appropriate security is maintained.
- have appropriate monitoring and auditing procedures in place; and
- be ready to respond to any failure to adhere to a data sharing agreement swiftly and effectively.

When personal data is shared, it is good practice for the organisation disclosing it to make sure that it will continue to be protected with adequate security by any other organisations that will have access to it. The organisation disclosing the information should ensure that the receiving organisation understands the nature and sensitivity of the information. It is good practice to take reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved in a data sharing agreement. Please note, though, that the organisations the data is disclosed to will take on their own legal responsibilities in respect of the data, including its security.

Difficulties can arise when the organisations involved have different standards of security and security cultures or use different protective marking systems. It can also be difficult to establish common security standards where there are differences in organisations' IT systems and procedures. Any such problems should be resolved before any personal data is shared.

There should be clear instructions about the security steps which need to be followed when sharing information by a variety of methods, for example phone, fax, email or face to face.

Governance

Responsibility

The various organisations involved in a data sharing initiative will each have their own responsibilities, and liabilities, in respect of the data they disclose or have received. The issues the data sharing is intended to address may be very sensitive ones, and the decisions staff members may have to take can call for great experience and sound judgement. Therefore, it is good practice for a senior, experienced person in each of the organisations involved in the sharing to take on overall responsibility for information governance, ensuring compliance with the law, and providing advice to staff faced with making decisions about data sharing.

Data sharing agreements

Data sharing agreements – sometimes known as 'data sharing protocols' – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

A data sharing agreement should, at least, document the following issues:

- the purpose, or purposes, of the sharing.
- the potential recipients or types of recipients and the circumstances in which they will have access.
- the data to be shared.
- data quality – accuracy, relevance, usability etc.
- data security.
- retention of shared data.
- individuals' rights – procedures for dealing with access requests, queries, and complaints.
- review of effectiveness/termination of the sharing agreement; and
- sanctions for failure to comply with the agreement or breaches by individual staff.

Data Protection Impact Assessments (DPIAs)

Before entering any data sharing arrangement, it is good practice to carry out a privacy impact assessment. This will help you to assess the benefits that the data sharing might bring to individuals or society more widely. It will also help you to assess any risks or potential negative effects, such as an erosion of personal privacy, or the likelihood of damage, distress or embarrassment being caused to individuals. As well as harm to individuals, you may wish to consider potential harm to your

organisation's reputation which may arise if data is shared inappropriately, or not shared when it should be.

Data standards

It is important to have procedures in place to maintain the quality of the personal data we hold, especially when we intend to share data. When we are planning to share data with another organisation, we need to consider all the data quality implications.

When sharing information, you should consider the following issues:

- **Make sure that the format of the data you share is compatible with the systems used by both organisations.**

Different organisations may use very different IT systems, with different hardware and software and different procedures for its use.

This means that it can be very difficult to 'join' systems together to share personal data properly. These technical issues need to be given due weight when deciding whether, or how, to share personal data.

Organisations may also record the same information in different ways which could lead to records being mismatched or becoming corrupted. There is a risk that this will cause detriment to individuals if holding an incomplete record means that you do not provide services correctly. Before sharing information, you must make sure that the organisations involved have a common way of recording key information.

- **Check that the information you are sharing is accurate before you share it.**

Before you share data, you should take steps to check its accuracy.

It is good practice to check from time to time whether the information being shared is of good quality. For example, a sample of records could be looked at to make sure the information contained in them is being kept up to date. The larger the scale of the data sharing, the more rigorous the sampling exercise should be. It is a good idea to show the records to the people they are about so that the quality of information on them can be checked. Although this may only reveal deficiencies in a particular record, it could indicate wider systemic failure that can then be addressed.

- **Establish ways for making sure inaccurate data is corrected by all the organisations holding it.**

You should ensure that procedures are in place for amending data after it has been shared. This might be because the data subject notifies you of an inaccuracy, or because they have asked you to update their details. The action you need to take will depend on the circumstances of each case. If the data is intended for ongoing use, then it could be necessary for all the organisations holding it to amend it.

- **Agree common retention periods and deletion arrangements for the data you send and receive.**

The various organisations sharing personal data should have an agreement about what should happen once the need to use the data has passed. Where the information is held electronically the information should be deleted, and a formal note of the deletion should be sent. Where the issue that the data sharing was intended to deal with has been resolved, all the organisations involved

should delete their copies of the information unless there is a requirement to retain it for another purpose, for example archiving. Paper records can cause problems. It can be easy to overlook the presence of old paper records in archives or filing systems – and they may well contain personal data subject to the GDPR. Once the need to retain them has passed, paper records should be securely destroyed or returned to the organisation they came from.

The various organisations involved in a data sharing initiative may need to set their own retention periods for information, perhaps because they work to different statutory retention periods.

However, if shared data is no longer needed for the purpose for which it was shared, then all the organisations it was shared with should delete it. However, the organisation, or organisations, that collected the data in the first place may be able, or be required, to retain the original data for another legitimate purpose.

Some information will be subject to a statutory retention period, and this must be adhered to. You must make sure that any organisation that has a copy of the information also deletes it in accordance with statute.

If you can remove all identifying information from a dataset so that it no longer constitutes personal data, then it can be retained indefinitely.

- **Train your staff so that they know who has the authority to share personal data, and in what circumstances this can take place.**

It is essential to provide training on data sharing to staff that are likely to make significant decisions about data sharing or have access to shared data. The nature of the training will depend on their role in respect of the sharing of personal data. It can be incorporated into any training you already give on data protection, security, or legal obligations of staff.

Different types of staff involved in data sharing will have different training needs, depending on their role. Those who:

- plan and make decisions about systematic sharing.
- administer systems; or
- make decisions in one off situations.

will each have different requirements based on their responsibilities.

The focus of the training should be enabling staff to make informed decisions about whether or how to share data, and how to treat the data they are responsible for.

People who have overall responsibility for data sharing need to understand:

- the relevant law surrounding data sharing, including the GDPR.
- any relevant professional guidance or ethical rules.
- data sharing agreements and the need to review them.
- how different information systems work together.
- security and authorising access to systems holding shared data.
- how to conduct data quality checks; and
- retention periods for shared data.

They also need the seniority and influence to make authoritative decisions about data sharing.

Reviewing your data sharing arrangements

Once you have a data sharing arrangement in place you should review it on a regular basis. This is because changes can happen, and they need to be reflected in your arrangements to ensure that such sharing can still be justified. If it cannot be justified, it should stop.

You should ask yourself the following key questions regularly:

- Is the data still needed? You may find that the aim of the data sharing has been achieved and that no further sharing is necessary. On the other hand, you may find that the data sharing is making no impact upon your aim and therefore the sharing is no longer justified.

- Do your privacy notice and any data sharing agreements you have in place still explain the data sharing you are carrying out accurately? Please see the fairness and transparency section of this code for further information.

- Are your data security and protection procedures still adequate and working in practice? All the organisations involved in the sharing should check:
  - whether it is necessary to share personal data at all, or whether anonymized/pseudonymized information could be used instead.
  - that only the minimum amount of data is being shared and that the minimum number of organisations, and their staff members, have access to it.
  - that the data shared is still of appropriate quality.
  - that retention periods are still being applied correctly by all the organisations involved in the sharing.
  - that all the organisations involved in the sharing have attained and are maintaining an appropriate level of security; and
  - that staff are properly trained and are aware of their responsibilities in respect of any shared data they have access to.
- Have you checked that you are still providing people with access to all the information they're entitled to, and that you're making it easy for them to access their shared personal data?
- Have you checked that you are responding to people's queries and complaints properly and are analysing them to make improvements to your data sharing arrangements?
- If significant changes are going to be made to your data sharing arrangements, then those changes need to be publicised appropriately. This can be done by updating websites, sending emails directly to people or, if appropriate, placing advertisements in local newspapers.

Things to avoid.

When sharing personal data there are some practices that you should avoid. These practices could lead to regulatory action:

- Misleading individuals about whether you intend to share their information. For example, not telling individuals you intend to share their personal data because you think they may object.
- Sharing excessive or irrelevant information about people. For example, routinely sharing details about individuals that are not relevant to the purpose that the information is being shared for.
- Sharing personal data when there is no need to do so – for example where anonymised statistical information can be used to plan service provision.
- Not taking reasonable steps to ensure that information is accurate and up to date before you share it. For example, failing to update address details before sharing information, leading to individuals being pursued at the wrong address or missing out on important information.

- Using incompatible information systems to share personal data, resulting in the loss, corruption, or degradation of the data.
- Having inappropriate security measures in place, leading to loss or unauthorised disclosure of personal details. For example, sending personal data between organisations on an unencrypted memory stick which is then lost or faxing sensitive personal data to a general office number.

Data sharing agreements

Data Security and Protection:

Your agreement should also deal with the main practical problems that may arise when sharing personal data. This should ensure that all organisations involved in the sharing:

- have detailed advice about which datasets may be shared, to prevent irrelevant or excessive information being disclosed.
- make sure that the data being shared is accurate, for example by requiring a periodic sampling exercise.
- are using compatible datasets and are recording data in the same way. The agreement could include examples showing how particular data items – for example dates of birth – should be recorded.
- have common rules for the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules.
- have common technical and organisational security arrangements, including for the transmission of the data and procedures for dealing with any breach of the agreement.
- have procedures for dealing with DPA access requests, or complaints or queries, from members of the public.
- have a timescale for assessing the ongoing effectiveness of the data sharing initiative and of the agreement that governs it; and
- have procedures for dealing with the termination of the data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it originally.

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis.

Is the sharing justified?

- Key points to consider:
- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.

- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share. (for example, was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Data sharing checklist – one off requests
Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?
Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the GDPR to share?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share. (for example, was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision.

Record your data sharing decision and your reasoning – whether you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.

Whether the information was shared with or without consent.

Signed:  Date:

Chief Executive
Volunteer Cornwall

Due Review: 04/2025