Association of Independent Museums

Helping Heritage Organisations Prosper

Success Guide

Successfully managing privacy and data regulations in small museums

Association of Independent Museums

Helping Heritage Organisations Prosper

Success Guide

Successfully managing privacy and data regulations in small museums

By Helen Shone
Development Partners

development partners

Contents

Who is this guide for? 1

Why are we talking about this now? 3

Why are you collecting data? 4
Only collect the information you need 4
Only keep data for as long as you need it 5

How are you collecting and storing data? 6
Where are your collection points? 6
How do you store your data? 6

When do you need consent? 8
Legitimate Interest: What is this all about? 8
Data Processing Activities: Consent versus Legitimate Interest 8
At which point should you gather consent? 12
Opt in versus Opt out 12
What should a consent statement look like? 12

What is a privacy policy? 13
What should a privacy policy cover? 14
Publicising the Privacy Policy 15
What does this mean for your historical data? 15

ACTION CHECKLIST 16

Further information 18

About Development Partners 18

The GDPR applies to the whole UK, so this guide is suitable for all AIM members across the UK.

Who is this guide for?

This guide is intended for museums and other cultural organisations wanting to understand how they should be responding to current and forthcoming data protection regulation. It isn't a guide to everything in the Data Protection Act (DPA), or the impending General Data Protection Regulation (GDPR), but focuses instead on the most important areas for action now. The GDPR applies to the whole UK, so this guide is suitable for all AIM members across the UK.

Data protection regulations are far more wide-reaching than discussed here and we recommend reviewing the guidance given by the Information Commissioner's Office (ICO) and by other organisations listed in the further reading section. The information given here is based on guidance currently available, and readers should be aware that further updates will be published by the ICO and Fundraising Regulator.

This guide is for trustees, senior staff and members of staff and volunteers involved in fundraising or marketing. However, it would be useful to share the key points with all staff and volunteers since so many of them will come into contact with data collection and processing in the course of their working week. Remember that data protection is not just a fundraising issue, it relates to any data that the organisation collects and uses, from admissions and gift aid declarations to mailing lists and volunteer information.

This guide will outline the main data protection issues to help you carry out an audit of your current position and draw up an action plan. It aims to be a practical guide that will put you on the right path for data protection compliance.

There is an action checklist included, which summarises the issues you need to consider and the action you may need to take.

What about our collections and archives?

Many heritage organisations will hold personal data in their collection and archives. At the time of writing the situation in relation to collections and archives is being clarified and the guide will be updated when more is known. The 1998 data protection act contained an exemption for archival records and it is expected that something similar will be included in the new legislation or guidance.

Once the relevant legislation is published, Collections Trust plan to update their sample acquisition forms to reflect the GDPR requirements and provide other advice relevant to collections. AIM will update this guide with the relevant links, as more information is known.

Why are we talking about this now?

The Data Protection Act (DPA) has been in force since 1998 and this has always required organisations to manage data fairly and responsibly. But this regulation is now to be updated and tightened in the EU's General Data Protection Regulation (GDPR), due to become law on 25 May 2018. The ICO is raising awareness of what is changing, but in doing so has also shone a light on what organisations should already have in place.

Enforcement action taken by the ICO in late 2016 and early 2017 has demonstrated the reputational and financial penalty for getting things wrong: 13 charities were fined for actions relating to wealth screening, data sharing and data appending - practices often considered commonplace in the charity world.

The connecting factor in all of these ICO cases was the issue of consent. The ICO stated that the activities themselves were not illegal; the problem was that they had not informed people that they planned to do these things with their data, and so people did not have the opportunity to object. In all cases, the organisations had consent statements and privacy notices in place, but the ICO ruled that they had not been sufficiently clear in these about how they would be using their supporters' data. This stricter interpretation of the DPA is a precursor to the changes to be found in the more rigorous GDPR.

Recent, stricter enforcement action, coupled with a general shift in attitudes to personal data, is seeing a move away from the laissez-faire towards a time of greater personal control and organisational accountability. It is really important that these changes are understood at the top of your organisation. Trustees and senior staff should not be 'protected' from these issues as they are accountable for the decisions made.

Organisations need to prepare for the changes to data protection law before the new regulations come into force on 25 May 2018. The new regulations will apply even though the UK will be leaving the European Union.

Why are you collecting data?

In the past many organisations have collected data simply because they have had the opportunity, and not because they knew how they would use it. A simple piece of advice is to be mindful and strategic about the data that is collected - be clear why it is that you are collecting data and what you plan to do with it. Document your decisions: the GDPR's accountability principle requires organisations to be able to show how they comply with data protection regulation, meaning that a record of your decision-making must be kept.

You may wish to collect personal data for a wide range of purposes, with some of the most common being:

- Newsletter mailings
- Fundraising appeals
- Volunteer management
- Events
- Gift Aid

Only collect the information you need

The DPA says that: 'Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.' This means that you should only collect data that is useful and avoid extraneous information that is irrelevant to your purposes. This also creates a smaller workload for data cleaning and management.

Document your decisions: the GDPR's accountability principle requires organisations to be able to show how they comply with data protection regulation

Data which is classified as 'sensitive' should be kept only under strictly controlled circumstances - this relates to racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences. For collecting sensitive data, one of the following criteria must be met:

- The individual has given explicit consent (eg they may have told you about a disability and how this might affect them at an event)
- The individual has made the information deliberately public
- To comply with the law
- For medical purposes
- For monitoring equality of opportunity

Remember that everyone has the right to request access to the data that you hold, so keep it objective and don't record anything that could jeopardise your reputation. It can be helpful to imagine the data subject standing behind you when entering their information on the database.

Only keep data for as long as you need it

Don't allow personal data to sit around indefinitely. It is tempting to keep hold of the data 'just in case' it is useful, but as the information gets older it becomes less of an asset and more of a liability. As time passes, it becomes more difficult to ensure that information is accurate, increasing the risk that outdated information will be used in error. Holding on to old data also increases the data burden: it must still be kept securely despite the fact that it is not useful, and the organisation must respond to subject access requests, even though you haven't been using it.

Although no absolute time-scale is given by the DPA, it states that personal data 'shall not be kept for longer than is necessary'. You need to set your own internal rules about how long this should be but there is probably little point in sitting on data that has been dormant for many years.

Be aware that there may be information that is needed for a long period for statutory or reporting reasons; Gift Aid records, for example, must be kept for six years after the relevant accounting period. Where appropriate, it is perfectly acceptable to create a skeleton record which keeps certain data fields active for a longer period than other superfluous details.

Having set your internal rules, this should be documented in a simple data retention policy, and a system set up to ensure it is implemented. It may be a challenge initially to identify and delete old data (which may be sitting in paper files as well as spreadsheets and databases), but a one-off effort to get the organisation to a sensible data retention position will pay off in the longer term.

How are you collecting and storing data?

The next step in your data audit is to consider how you are collecting your data and how you are storing it.

Where are your collection points?

Most organisations collect data from a number of different sources. These touch points could be:

- Visitor reception
- Online donations
- Friends group
- Newsletter sign up
- Gift Aid data
- Events
- Commercial hire
- Retail
- Volunteer management systems

Organisations need to be consistent in their approach to gaining consent wherever it is collected. This is important for your supporters' experience, but even more so for back office systems which support your activities - it is very difficult to keep good records on consent if you are asking different questions in different places.

Think through the different places that you collect data and consider whether the approach to gaining consent is streamlined.

It doesn't matter if the systems are paper-based in one area of the site and electronic in another, but the main consent statement and options need to be aligned.

More information on consent is provided in the sections below.

How do you store your data?

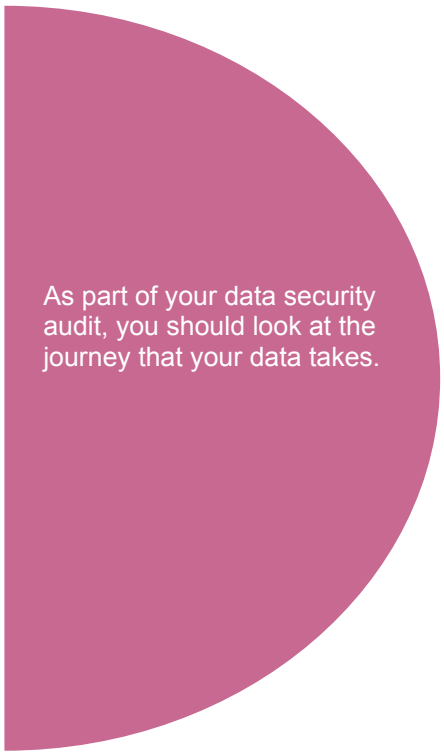
Currently, there are two main data protection issues when it comes to data storage. The first is security, which has always been a requirement under the DPA, and the second is the ability to store consent information in the way that is required under GDPR.

The DPA has the following requirement regarding security:

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'

Databases tend to be more secure than paper-based systems and spreadsheets. They are independent of a computer network's main shared documents and require passwords to log in. Typically, access is limited to those who need it. Risk areas include (though are not limited to) a large number of people having access to the database, lack of suitable data back up process, and data reports downloaded onto the main computer shared drive where anyone can access them. Security should be reviewed periodically to ensure that you are reducing the risk of any data breach.

Organisations need to be consistent in their approach to gaining consent wherever it is collected.



It is not a requirement to have a database to manage your data - a paper-based or spreadsheet system is fine if this is proportionate to the amount of data you hold and process. But security of these systems must also be reviewed on a regular basis, and procedures put in place to mitigate any security risk. You must document your decision-making and actions.

As part of your data security audit, you should look at the journey that your data takes. If you input straight onto a database, then it is a very short one, but not all systems are this high-tech. An example scenario at a small museum could be as follows:

Visitors fill in a paper form at reception on arrival. The form is passed on to an administrative member of staff or volunteer who puts the data onto a spreadsheet.

Risk points could be:

- The form is left unsupervised on the visitor reception desk.
- The form is not shredded or appropriately filed away after the information is put onto the data spreadsheet.
- The data spreadsheet can be accessed by all staff and volunteers who have access to the shared computer network.

All of the above outcomes could lead to information getting into the hands of people inside or outside the organisation who have no right to access it.

Mitigation of these risks could be:

- A lockable drawer at reception to keep forms in when the desk is unsupervised.
- A system of shredding is put in place for forms that have been processed.
- The data spreadsheet or the relevant area of the computer network is password protected, with only appropriate people given access.

Storing Consent Data

The new data protection regulations represented by GDPR require organisations to gather and record more information relating to consent than under the DPA. As the new regulations state that consent cannot be assumed to last forever, they require organisations to record the date that consent was given. And if a supporter subsequently 'opts out' it will be necessary to record the date of this too. The rules also require organisations to offer supporters the option to opt in or out of different communication channels, such as post, email, phone and SMS.

As you can imagine, the combination of these requirements necessitates a large number of new fields in your databases or columns in the spreadsheets. To date, most databases have not been automatically configured to support these new requirements and so a 'work around' has to be found, using fields that you can 'query' or search as needed. This system needs to be in place and ready for use by May 2018 at the latest when GDPR comes into force.

When do you need consent?

Data processing refers not just to the communications that you send out, but also to the range of ways that you may use personal data, from analysis of visitor statistics to wealth screening. Some of these activities are considered more 'intrusive' (to use the ICO's description) and therefore there is a greater requirement for consent to carry them out. Others can be carried out on the basis of 'legitimate interest' described below.

Legitimate Interest: What is this all about?

Legitimate interest is the alternative legal basis for charities to carry out certain types of data processing. Organisations must balance their interests to process personal data to meet their objectives against the rights of the individual. The outcome of this balancing test determines whether personal data can be processed without needing consent.

In relation to direct marketing by post and phone (email and SMS always requires consent), the regulation requires organisations to consider the 'reasonable expectations' of individuals based on their relationship with you. If the individuals in question do not have a relationship with you and would be surprised to receive a mailing, then it is likely that the balancing act would not be in your favour. In addition, you should consider the frequency of the mailings you are sending - for instance, the individuals concerned may feel that monthly mailings are unreasonable, but may be happy to receive an annual update.

When you are relying on legitimate interest as your basis for a mailing, then you must always provide a prominent and easy step for opting out of future direct mail. And remember that once someone has opted out, the legitimate interest rule cannot be used, so you must find a way to exclude them from your future mailings.

Under GDPR, public bodies (including local authority museums) will no longer be able to rely on legitimate interest as a legal basis for data processing without consent. Instead, they will need to be able to show that 'the processing is necessary for the performance of a task carried out in the public interest' or 'for the performance of a contract with the data subject'.

Data Processing Activities: Consent versus Legitimate Interest

Performance of a Contract / Service Communications
When someone buys event tickets or orders something from your online shop, they expect to receive confirmation in the same way that they made the transaction - ie by email if sent by email or submitted online, or by post if sent by post. This type of confirmation is not designated a direct marketing activity and can take place without consent.

The Privacy and Electronic Communications Regulations (PECR) make an exemption in terms of email consent for further follow up communications to this type of commercial activity. You may send information that is directly relevant to the first communication without opt in consent. So someone who buys an event ticket and provides an email address for the processing can be sent information about other events, and someone who buys something in the online shop can be sent emails about other products - but in both cases you cannot add them to a general mailing list. You must always provide an opportunity to opt out of these emails.

Aggregate data

Analysis of aggregate data is considered unobtrusive as you are not looking at one individual's behaviour, but at the group as a whole. Consent is not needed.

Direct Marketing

Any mailings which further the aims and objectives of an organisation are considered direct marketing. This includes bespoke letters, which can be surprising as we tend to think of direct marketing as something sent to large numbers of people. It means that almost all types of communication with supporters need to be covered either by consent or (for mailings by post) the legitimate interests rule.

Wealth Screening and Research

Wealth screening (the practice of analysing data to estimate an individual's capacity to give) and individual research profiles are considered by the ICO to be intrusive data processing activities. They are not illegal, but require consent. It is important that these activities are not hidden in the privacy policy under ambiguous terms such as 'research', which could mean any number of different activities.

There has been much discussion regarding the question of prospect research; historically, a certain amount of research has been carried out at the initial stages of a relationship, before consent has been established. There has been a widely-held understanding that information in the public domain can be accessed and used to create a profile, with the usual caveats about the reliability of the sources.

At a landmark conference in February 2017 on 'Fundraising and regulatory compliance', the ICO made it clear that 'business as usual' is no defence for continuing this practice. It is the ICO's view that information in the public domain given by individuals for a specific purpose should not be 'fair game'.

This is a conundrum for major gift fundraisers. They have used this research to ensure that prospects are approached with an area of interest that is most appropriate and in the way most suited to them. Indeed, many high net worth individuals have come to expect this level of research as part of the process. On the other side of the coin, it is also important for ensuring that the organisation uses resources in the most prudent way. Debate continues on exactly what is acceptable before consent has been established, and if this is an area that affects you, then it is recommended that you look out for the latest information. The Institute of Fundraising is a reliable source and there are discussion forums on LinkedIn.

Data Sharing

The concept of data sharing covers a wide range of activities, some of which are likely to require consent and some which can be covered by the legitimate interests rule.

All of the ways in which you share data with a third party should be spelt out in your privacy policy, even when this is needed to carry out your day to day activities, such as use of a mailing house for a newsletter. Data sharing should always be carried out with a contract in place as you retain responsibility for what the third party organisation does with the data. You need to check their data protection credentials and ensure that they are up to scratch before sharing.

Consent is required when people might not have reasonably expected a type of data sharing to take place. An example of this would be when data is shared with a commercial organisation or when it is shared with a charity which does not have the same objectives. It is also inadvisable to share data for wealth screening without explicit consent as the ICO states that they consider it 'highly unlikely' that legitimate interest would apply.

Giving your data to another charity for their own use is to be avoided. An example which often crops up is of a local organisation wanting to use your mailing list to send information about their activities directly to your supporters. The ICO has ruled that sharing data with another organisation in this way can be harmful to an individual's interests as it multiplies the direct mail they may receive. Such data sharing may not be justifiable under legitimate interests, meaning consent must be established before it takes place.

Employee and Volunteer records

This data can be processed under the legitimate interests rule. The ICO has specific guidance for employee data, which is also relevant for volunteers. It is available here:

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Membership / Friends

When people sign up to membership or a Friends scheme, they automatically provide their contact details. If their data has been captured purely for the membership scheme, without a general opt in request, then you are restricting your data processing activities for which you have consent to those compatible with membership. However, since these people are clearly engaged with the museum, you may be able to use the legitimate interest grounds for non-membership communications by post.

One of the stated benefits of a membership or Friends scheme is usually a magazine or newsletter, and this falls into the 'performance of a contract' category. This may be sent by email (if they have given you their email address as part of the membership sign up) or post. However, what is a grey area is the content of this newsletter. Would the recipient reasonably expect this to include fundraising appeals? If members opted in to a broad consent statement and a link to the privacy policy, then this would not need to be a concern.

If your Friends scheme is run by a separate charity, they too will need to abide by data protection regulations and have their own privacy policy. You may wish to support the Friends' trustees in their own process to becoming compliant as the reputation of the parent museum will be harmed by any data breach.

Separate Friends organisations cannot automatically share their data with the parent museum. A legitimate interest 'balancing test' should be carried out to ensure that this would be expected by members and not harm the interests of the individuals. The data sharing between the two organisations and how it will be subsequently processed should be spelt out in the privacy policy of both.

ACTIVITY	CONSENT NEEDED NO	YES	LEGITIMATE INTEREST
Performance of a Contract - ie. confirmation of an order or event ticket	✓		✓
Analysis of aggregate data eg visitor statistics, event attendees or fundraising	✓		✓
Employee and volunteer records	✓		✓
Direct Marketing by Post or Phone	✓		✓
Donation thank you letter	✓		✓
Direct Marketing by Email, SMS, Automated Phone Calls		✓	
Detailed research profiles created in-house or externally sourced		✓	
Wealth Screening		✓	
Sharing Data (depends on type)		✓	✓

An Example:

For a Friends or membership scheme which is part of the museum or heritage organisation: it is advisable to have a general consent statement which includes other mailings from the museum, and a link to the privacy policy. This should be opt in consent for mail / email, and then you can record people's contact preferences accordingly.

If you ask people to opt out rather than opt in, you will not have consent as defined by GDPR, and any data processing will have to be on 'legitimate interest' grounds. You will not be able to email except to meet the expectations of the membership benefits eg. if your membership newsletter is by email.

If the Friends group is a separate charity: the Friends organisation must make it clear that it is separate from the museum when signing up new members. If they will share the data with the museum, this must be explicitly referred to in the privacy policy and a legitimate interests balancing exercise must be carried out to ascertain whether this is appropriate.

Safest is a system where members give consent on sign up, linked to a privacy policy which outlines all of the data processing activities. For existing Friends you need to review the consent that you already have and decide whether it is sufficient to meet the GDPR requirements - see section on historical data below.

At which point should you gather consent?

The ICO and Fundraising Regulator recommend that consent to hold and process data is gained when data is first collected. This is normally achieved through the combination of a consent statement (which gives the main points) and a privacy notice (which gives the detail). Held together, these two should cover all of your data processing activities.

When it is not possible to gain consent at the point of data collection, then it should be at the first available opportunity, such as the first time you make contact with them. It is considered unacceptable to sit on names and addresses without consent just because you are not using them.

Opt in versus Opt out

Under the DPA, it has been acceptable to require supporters to 'opt out' of various forms of data processing, such as being added to a mailing list, rather than to 'opt in'. Typically, there would be a statement saying something along the lines of the following: 'If you are not happy for us to send you further information about our activities, please tick the box.'

The rules for email, SMS and automated phone calls have differed from other forms of communication since 2003, when separate legislation (PECR) required consent to be on an opt in basis. So since 2003 we have had opt out for post, normal phone calls and other areas of data processing and opt in for email, SMS and automated phone calls.

Under GDPR, consent for all forms of data processing and communication should be opt in. The new requirement is that consent must be freely given, specific, informed and unambiguous. Individuals must show a proactive choice; consent cannot be assumed from pre-ticked boxes or inactivity. Information about data processing must be explained in a way that people can easily understand, and not hidden in jargon or ambiguity. Individuals should have the opportunity to opt in to different channels of communication (post, email etc), rather than be expected to sign up for all of them in one.

What should a consent statement look like?

The consent statement needs to tell people the basics about what you will be doing with their data, and link to the more detailed privacy policy. It should be short enough that people will read and understand it, but long enough for it to be meaningful. Don't use more formal language than usual - it is much better to adopt the same kind of tone that you use in your other communications. And since you are asking people to pro-actively opt in, aim to be engaging so that they want to sign up. Try to think of something inspiring and unique to you. It is good practice to remind people that they can subsequently opt out at any time.

- Use house style
- Be interesting, engaging
- Offer different communication channels, not just a single YES / NO choice
- Be consistent across all data collection locations and mediums
- Ensure your statement is not ambiguous
- Remind people they can subsequently opt out
- Provide a link to your privacy policy

An example of the bare bones:

We would love to keep in touch with you about our news, activities and fundraising appeals. You can opt out at any time. If you agree to being contacted, please tick the following boxes:

- Post
- Email
- Phone
- SMS

Full details of how we look after our supporters' data are available in our privacy policy.

Consent doesn't have to be given through a tick box or a written statement. It can be oral or via another act which demonstrates an individual's wish to opt in - for example a business card dropped into a box when it is made very clear what the card will be used for. But where consent is not written, it is best practice to confirm in writing and provide a link to the privacy policy.

What is a privacy policy?

The privacy policy (sometimes called a privacy notice or fair processing information) is probably your most important document relating to data protection. Despite the fact that it has been a long-term requirement under data regulations, many small charitable organisations still do not have one. This can be quickly and easily rectified and should be prioritised by any organisations that find themselves in this position.

The privacy policy should be a clear explanation of who you are and what it is that you will do with an individual's data. It should cover all of your current data processing activities and attempt to future-proof against your future data processing needs, otherwise there is a risk that you will find yourselves unable to do something important at a future date.

Some examples of clear privacy policies include:
National Museums of Scotland - https://www.nms.ac.uk/privacy-notice/

RNLI - https://rnli.org/footer/privacy-and-security

Cancer Research - http://www.cancerresearchuk.org/privacy-statement

However at the time of publishing this guide, these statements may not have been updated to reflect all of the new GDPR requirements.

It is acceptable to update privacy policies as long as they are readily accessible, but if there is a major change it will be necessary to actively bring this to the attention of your supporters.

It is acceptable to update privacy policies as long as they are readily accessible, but if there is a major change it will be necessary to actively bring this to the attention of your supporters.

What should a privacy policy cover?

In a way, this should be a summary of everything we discussed in this document. Remember that you must be specific, clear and unambiguous in describing your data processing activities. It must be easy for non-specialist audiences to understand what it is that you will be doing with their data. It is accepted practice to write in long-hand where needed, using a whole paragraph to explain one area of data processing if this is the best way to avoid ambiguity. You can also have a list of bullet points if this seems the best way to get your information across, but remember that clarity is prized more highly than brevity. Headings to include, where relevant, are:

- Who you are, including your charity number and address
- What personal data you collect
- What you will do with the data, examples include -
    - ✓ Mailings relating to news and events
    - ✓ Fundraising appeals
    - ✓ Research (be specific about the type of research you will carry out)
    - ✓ Wealth screening (explain what this is and how you will do it)
    - ✓ Aggregate data analysis, which could include monitoring visitor statistics or the effectiveness of communications, including email tracking
    - ✓ Data sharing - who you will share it with and for what purposes
- Cookies on your website
- How you will store the data and keep it secure
- How people can submit a 'Subject Access Request'
- A statement regarding updates to your privacy policy, 'We regularly review our privacy policy and may make changes from time to time.'
- The date of the latest update to the privacy policy.
- How to get in touch

The Subject Access Request is a legal requirement that all organisations must fulfil if requested. This refers to an individual's right to see a copy of the information an organisation holds on them. This includes an entitlement to be:

- told whether any personal data is being processed
- given a description of the data, the reasons it is processed and whether it will be shared
- given the source of the data

Under GDPR you may no longer charge a fee unless the request is 'manifestly unfounded or excessive' or if the individual makes multiple requests.

Publicising the Privacy Policy

Don't just write a privacy policy and leave it to gather dust on your desk. You need to share it with your supporters and make it easy to find.

It is usual to have a web page dedicated to the privacy policy. Links to it can then be situated as a footer on your website (so that you can link to it from any page) and as a footer in your emails.

If you are producing a privacy policy for the first time, you should inform supporters, perhaps through your newsletter, magazine or other regular mailing.
It may not feel like the most interesting thing in the world to be promoting, but it is important for you to be able to demonstrate that you have made efforts to share this information.

Be prepared to manage people opting out of different elements of your privacy policy. They may say that they are happy to receive newsletters, but don't want to receive appeal mailings, for instance. Or they may say that they don't want you to research or wealth screen them.

What does this mean for your historical data?

Most organisations have data relating to the old system of 'opt out', and some may have no consent records at all. Can this be unlocked? Some major charities have decided to write to everyone on their database and ask them to pro-actively opt in (eg. RNLI) knowing that they will lose a large percentage of their database. Their 'up side' to this decision is that they will have a far more active database at the end of the process, knowing that everyone is engaged with the cause, and they will have reduced direct mail costs.

If you choose to take this approach, you will know that you are completely covered, but it would be likely to come at a sizable cost to your database. If you want to continue to use your data as it is, you will need to look at it in detail, review the consents that exist, the sensitivity of the data and assess the risks.

A main consideration is whether you plan to make contact by email or post, which can be summarised as follows:

Email contact - you can only contact those people who have actively opted in. Proof can be through opt in to a consent statement or through signing up to an email newsletter or other email specific communication (though the latter cases would be specific to that particular communication unless they were asked to opt in to all email communications at the time). You cannot unlock email addresses for which you hold no consent - the ICO says, 'Note that organisations cannot email or text an individual to ask for consent to future marketing messages. That email or text is in itself sent for the purposes of direct marketing, and so is subject to the same rules…'

Post contact - you can choose to rely on the legitimate interest rule to continue to make contact via post. There is a particularly strong case for those people who were offered an 'opt out' consent statement and did not opt out, as you can argue that they would be likely to expect to receive your mailings. You may choose to contact people by post to ask them to upgrade their consent status to 'opt in', but note that anybody who does not reply to such a request after GDPR is in force must be assumed to have opted out, and their records amended accordingly.

Don't just write a privacy policy and leave it to gather dust on your desk.
You need to share it with your supporters and make it easy to find.

ACTION CHECKLIST

All of your data protection decision-making should be documented through the minutes of trustee or internal meetings or in policy documents. This is so that you can show what actions you have taken to ensure you comply with regulations if complaints are made or you are audited by the ICO.

- Assess your data collection needs against the data you are collecting. Are you collecting more than is necessary? Can you get rid of data that is not needed?
- How long do you need to keep your data? Create a data retention policy and implement it.
- Where and how are you collecting data? Are you consistent?
- Security: Are your data collection and storage systems secure?
- What changes do you need to make to your database or other systems to record consent dates, as needed when GDPR comes into force?
- What data processing activities are you carrying out?
- What consent do you have to carry these out?
- Will you rely on the legitimate interest rule for some activities? If so, document why you consider this reasonable.
- How will you update your consent statement?
- Do you have a privacy policy? If not, create one. If you do, review it carefully.
- Newly created privacy policies should be publicised - how will you do this?
- What are your plans for your historical data?

Further information

- Institute of Fundraising: GDPR: The Essentials for Fundraising Organisations http://www.institute-of-fundraising.org.uk/guidance/research/gdpressentials/
- Arts Council England: A practical guide to lawful fundraising for arts and cultural organisations http://www.artscouncil.org.uk/document/practical-guide-lawful-fundraising
- Fundraising Regulator: The Code of Fundraising Practice https://www.fundraisingregulator.org.uk/code-of-fundraising-practice/code-of-fundraising-practice-v1-4-310717-docx/
- Fundraising Regulator: Personal Information and Fundraising: Consent, Purpose and Transparency (includes a checklist and toolkit) https://www.fundraisingregulator.org.uk/wp-content/uploads/2017/02/GuidanceFinal.pdf
- CO: Guide to data protection https://ico.org.uk/for-organisations/guide-to-data-protection/
- ICO: Privacy notices, transparency and control https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

About Development Partners

Development Partners is a fundraising and business development consultancy to the heritage and arts sector. With data protection expertise that relates specifically to this sector, we can cut through the jargon to provide sensible advice on the steps to compliance.

We work across the UK with organisations of all shapes and sizes from major museums to small volunteer-run heritage sites. Together we assess and capitalise on the unique opportunities of each organisation for building a stronger future.

Helen Shone

Development Partners Ltd

September 2017

development partners

Association of Independent Museums

Helping Heritage Organisations Prosper

Association of Independent Museums (AIM)
3 Chestnut Grove
Ludlow
Shropshire SY8 1TJ

AIM Editor – Sassy Hicks
www.aim-museums.co.uk

development partners