A Practical Guide to Lawful Fundraising for Arts and Cultural Organisations

Updated May 2018

Bates Wells Braithwaite

ARTS COUNCIL ENGLAND

A Practical Guide to Lawful Fundraising for Arts and Cultural Organisations

Introduction

Fundraising in the arts and cultural sector is changing. As many organisations become less reliant on state funding and foundation grants, they are exploring further and investing more in private fundraising and philanthropy.

As philanthropy becomes more important, having a sound understanding of the legal requirements of data protection law is essential in order to enable organisations to make best use of the information they hold and to benefit in full from the generosity and goodwill of their supporters and friends.

Everybody, from your trustees to your volunteers, should be an advocate for your organisation. They therefore need to understand the legal obligations and fully engage with data protection law and regulation. Arts Council England has commissioned this guidance to provide an understanding of the practical steps that must be taken to fundraise in a legally compliant manner and in accordance with best practice.

This information is accurate at the time of writing. Data protection law is constantly developing and the regulatory landscape is changing all the time. See section E below for detail on what is on the horizon. We recommend you check the Information Commissioner's website frequently for updates to data protection law and regulatory guidance.

Arts Council England will work with BWB to review and update this guide from time to time to reflect changes in law and regulation as they arise, so please check the website for the latest version. **This guide was updated in May 2018.**

BWB
Bates Wells Braithwaite

ARTS COUNCIL ENGLAND

Arts Council England is the national development body for arts and culture across England, working to enrich people's lives. We support a range of activities across the arts, museums and libraries – from theatre to visual art, reading to dance, music to literature, and crafts to collections. Great art and culture inspires us, brings us together and teaches us about ourselves and the world around us. In short, it makes life better. Between 2018 and 2022, we will invest £1.45 billion of public money from government and an estimated £860 million from the National Lottery to help create these experiences for as many people as possible across the country.www.artscouncil.org.uk.

CONTENTS

A: The legal framework and basic principles – An introduction

The legal rules can be found mainly in the General Data Protection Regulation, Data Protection Act 2018 and Privacy and Electronic Communications Regulations 2003 plus the Fundraising Code.

From 25 May 2018, the use of individuals' personal data will be governed primarily by the General Data Protection Regulation (**GDPR**). In the UK, this will be supplemented by the Data Protection Act 2018.

The potential implications and tasks associated with the incoming GDPR have been daunting for many organisations, and we have been seeing signs of a rush to compliance which may prove counter-productive. We suggest that appropriate planning is done before rushing out policies and communications - it is important to get it right. The Information Commissioner, Elizabeth Denham, has said that 25 May will *"merely mark the end of the beginning of a very long journey"*. The regulator has indicated that its aim will be to get organisations into compliance, rather than to punish those who are (not wilfully) behind.

The GDPR includes a number of obligations and requirements regarding the handling of personal data generally (e.g. in relation to security), and accountability generally (e.g. the appointment of data protection officers). This guide focusses only on those aspects of the GDPR related directly to your fundraising activity.

There are additional legal rules which apply to 'electronic Direct Marketing' (i.e. sending people marketing/ fundraising by electronic means such as phone, text and email) - these are the Privacy and Electronic Communications Regulations 2003 (**PECR**).

Who enforces these rules, and what if we get it wrong?

The ICO is the main UK regulator, with powers to issue significant fines – but the most damaging consequence to getting it wrong might be reputational harm and loss of trust with supporters, which could take a long time to rebuild.

These rules are enforced in the UK by the Information Commissioner's Office (**ICO**). The ICO is the UK's independent regulatory authority on data protection and information, reporting directly to Parliament. Its stated role is to uphold information rights in the public interest.

Charitable fundraising is also regulated by the Fundraising Regulator's Code of Fundraising Practice. The Code is a self-regulatory scheme which includes both legal requirements and expected professional standards. Self-regulatory means that those organisations who sign up agree to be bound by it. The Fundraising Regulator is an independent body which sets and maintains the standards for charitable fundraising. It regulates compliance with the Code and works closely with both the ICO and the Charity Commission.

For the most serious breaches of the GDPR, the ICO has powers to fine up to €20m or 4% of total worldwide annual turnover. Whilst we would expect the ICO to take a proportionate approach to any enforcement action (which may include fines but also includes providing guidance, or requesting that an organisation pause its processing activities until they are compliant), much greater harm, from a fundraising perspective, may come from the reputational harm and damage to the trust between organisation and supporter.

What is "Direct Marketing"?

Both the GDPR and PECR impose restrictions on Direct Marketing (defined below). The GDPR gives individuals a specific right to object to their personal data being used for it. Additionally, sending *electronic* Direct Marketing (e.g. text, email and telephone calls) can require prior consent under PECR. This is explained in more detail below. It is therefore important to understand what communications will be viewed as Direct Marketing.

Direct Marketing: the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

This guide deals with fundraising. Fundraising communications will always be regarded as Direct Marketing. However, Direct Marketing is interpreted widely by the ICO to capture all targeted promotional material and goes beyond fundraising messages, to include even the promotion of "aims and ideals" of a charitable organisation and communications about upcoming events and activities – i.e. newsletters will be considered to fall within this definition.

A communication will also be Direct Marketing if it is partly promotional, even if this is not its sole purpose, for instance an administrative message relating to a previous donation which would not be considered Direct Marketing, will become Direct Marketing if it also includes a solicitation for further support. The table below sets out some examples of communications which fall inside and outside the definition.

Message	**Is it Direct Marketing?**
An email newsletter to your supporter database with details of upcoming shows at your venue. Even if this is addressed to "dear all", this is Direct Marketing.	
Mail delivered to every house in an area, or adverts shown to every person who views a website. These are not Direct Marketing because they are not targeted at individuals.	
A short "thank you" email to a supporter, which may explain briefly what you have spent their money on. This will not be Direct Marketing, provided it does not also contain an ask for further support or details of your upcoming events/ exhibitions.	
A simple request to sign a gift aid declaration after an individual has made a donation to your organisation. Again this will not be considered as Direct Marketing provided it does not contain additional fundraising material.	
A telephone call with a customer to take a booking for a performance. This is not Direct Marketing – it is administering a contract.	
During the above call, the employee also asks for a donation. Though the main purpose of the call is for administration, as there is a marketing element, it still falls within the definition of Direct Marketing.	

The ICO's guidance on Direct Marketing can be found here. This has been updated to take account of GDPR.

Collecting and holding personal data: Privacy notices

There are broadly three key steps to ensuring your fundraising is compliant with data protection law and regulation:

1. Privacy Notices – providing information at the start of the "data journey".

2. Ensuring you have an appropriate legal basis for processing the data (do you need consent?).

3. Opt-outs – enabling and accommodating the individual's right to object to the processing of their data.

Steps 1 and 2 are crucial in order to develop a useable supporter database. You should ensure that you collect personal data in a compliant way from the very beginning, or at the start of the "data journey". This involves informing individuals of your intended use of the data, and obtaining any consent necessary for your anticipated fundraising activities.

This guide will explain what you need to tell somebody when you collect their personal data in different contexts (e.g. when selling a ticket to an event by phone, in person or online) and what permissions you require to fundraise via different channels (e.g. by post, telephone or email).

Fairness and transparency

The first principle of the GDPR requires that personal data is processed **fairly**, **lawfully** and in a **transparent** manner.

What should go in our privacy notices/ policies?

Part of the requirement to process **fairly** and **transparently** includes taking reasonable steps to provide the individual with certain Privacy Information. This is typically provided in a 'privacy notice' (sometimes also called a privacy policy or statement). Under GDPR, this must include as a minimum:

- the identity and contact details of the data controller and, where there is one, their data protection officer (the data protection officer will be the person in your organisation who is responsible for data protection compliance);

- an explanation of the purposes of the processing and legal basis for it;

- where the legal basis is the organisation's legitimate interests, an explanation of the legitimate interests pursued by the data controller;

- the categories of personal data involved;

- any recipients or categories of recipients with whom the personal data is likely to be shared;

- countries where the personal data may be transferred and the level of protection offered by those countries;

- how long the personal data will be kept for;

- the existence of the data subject's rights;
- the right to withdraw consent to processing at any time, where relevant;
- the right to make a complaint to the ICO;
- the source of the personal data (if not collected from the individual his or herself) and whether it came from publicly accessible sources ; and
- the existence of automated decision making, including profiling in relation to that data.

The aim should be for the privacy notice to be clear and transparent in explaining what it is you will do with a person's personal data. If you later want to do something which was not covered in the privacy notice or otherwise communicated to the individual then there is a risk you will be unable to do it. Thoughtfully prepared privacy notices are one of the most useful tools in a fundraiser's armoury.

When do we need to provide this?

This information needs to be provided at the point of data collection, or if the personal data is not collected from the individual directly, within a reasonable period of time (and within one month), or if sooner when the first communication with the individual takes place, or before the data is disclosed to another recipient.

But that won't all fit on one page!

Layering is a concept talked about under GPDR where you can use more than one document to provide the Privacy Information. Certain key privacy information is available immediately (in a first 'layer') and more detailed explanation is provided in a second 'layer', usually via a hyperlink to - or offering a hard copy of - your longer privacy notice.

Some of the things your privacy notice might typically include in the first layer, in order for the processing to be sufficiently fair and transparent, are:

- the identity and contact details of the data controller;
- an explanation of the purposes of the processing;
- the right to withdraw consent, where relevant;
- whether you will share the data with other organisations for their own purposes. For instance, you may be sharing with your own trading subsidiary, other organisations in your group or with particular arts and cultural organisations as part of a collaboration;
- whether you will use the data to create a financial profile of the individual, for instance to carry out wealth screening (see further below); and
- whether you will send the data to a country outside of the European Economic Area (e.g. if you are sharing with a partner in the US).

Privacy notices can be provided in writing (e.g. where data is obtained from an online or a paper donation form) or orally (in person or over the telephone):

Examples	Guidance
Telephone/ in person script "Thank you for booking tickets at Marlowe's Sphere. We would like to add your contact details to our supporter list so we can keep you informed about events and other developments at our venue and contact you to ask for support/ fundraise by [email/ SMS/ post/ telephone/ social media]. Is this alright?" You will also need to inform the individual of their right to opt-out or withdraw their consent, and tell them where they can find further information (e.g. in your privacy policy). Note that if you intend to share the data with other organisations, you will also need to tell individuals that you will do this. For more information see Audience Agency's guidance here.	These examples take an "opt-in" approach to obtaining consent for Direct Marketing by post. This is best practice **but is not a legal requirement for postal fundraising–** See below. You may send Direct Marketing communications to individuals by post without their consent (but remember consent is required for email marketing). However, if you choose to voluntarily give individuals the choice about whether to opt into receiving communications by post and the individual chooses not to tick the box for "post", then you cannot send that individual Direct Marketing by post.
Online/ paper form We are Marlowe's Sphere. We will add the contact details you provide to us to our supporter list so we can keep you informed about events and other developments at our venue and contact you to ask for support/ fundraise [by email/ by SMS/ by telephone call etc.). If you agree to being contacted this way, please tick the following boxes: Post❑ Email❑ Phone❑ SMS❑ [Social media❑] ***[note pre-ticked boxes should not be used]*** We respect your data and will use it in accordance with our privacy policy, which can be found [here/ online at] www.marlowesphere.com/privacy. If you would like to find out more or wish to stop receiving communications then please contact us on 020 1234 5678 or at info@marlowesphere.com.	Where organisations are undertaking wealth profiling/ screening, which we will explain in further detail below, the ICO has been clear that you must let data subjects know you will be doing so. We recommend including wording in your privacy notice to describe the wealth screening you are carrying out. Some example wording is set out below but the statement you use should be tailored to reflect the profiling that you are carrying out: *"We may use profiling and screening techniques to analyse your personal data and create a profile of your interests and preferences. In doing so we may make use of additional information about you, including where you live, your [age], [any other demographic information] and other information and measures of wealth, when it is available from external sources (such as public registers, online (including records that you have made public on social media) or the electoral roll). We may use third party suppliers to undertake these activities on our behalf.* *This helps us understand a bit more*

	*about the people who support us so that we can make appropriate requests to those who may be able and willing to give more than they already do, enabling us to raise funds sooner and in a more tailored way than we otherwise would."**
The written statement could also be prominently displayed at front-of-house in appropriate circumstances (though this will not be practical in all cases), and the telephone statement may be pre-recorded.	

**Please note you should always take specific advice on the statement you use to describe wealth screening, as what is required will depend on the nature of the wealth screening you are carrying out.*

See the ICO's "good and bad examples of privacy notices" here, and its guidance on "Privacy Notices under the EU GDPR" here.

What is consent?

In addition to **informing** the individual about how you will use their personal data, you must also ensure you have all necessary permissions to use the data to carry out your intended fundraising activities. Consent is not always necessary (or even appropriate), but is required for certain electronic forms of Direct Marketing, as explained in more detail below.

Consent is defined in the GDPR as:

Consent: any:

- freely given

- specific

- informed

- unambiguous indication of an individual's wishes by which he or she,

- by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The GDPR has 'raised the bar' for what constitutes valid consent. Whilst under the previous law, implied consent, or pre-ticked boxes, could be acceptable, valid consent must be unambiguous and expressed by a clear affirmative action.

Effectively this means that individuals must have **taken a clear action** to demonstrate their willingness for future contact, must **know what they are agreeing to** and must have a **clear understanding** of what you will do with their information.

This includes:

- consent should not be contained in other terms and conditions (i.e. not 'hidden away' in other information)

- it should not be bundled with a service

- it should be easy to withdraw

Consent should be granular (different purposes should not be bundled together).

Consent must also be **granular** i.e. give people more specific choice about the ways in which you will use their personal data – for example, providing the opportunity to opt-in to marketing (including fundraising) separately to opting-in to sharing with other organisations.

- **By channel**. A high degree of granularity will be required for the communication channels by which you envisage sending electronic fundraising communications (e.g. SMS, email, social media messages, but not post or live telephone calls – which do not require consent). The best practice is to provide a tick box opt-in to the sending of fundraising communications by phone, email, text and post. This approach makes it clearer to you which channels you can use to contact an individual.

- **By activity**. Whilst clear consent to each activity would be ideal, practically speaking this could be counterproductive if it means presenting a long list of activities as this could lead to 'click fatigue' and actually make the activities less clear. Organisations may take the approach of listing 3 to 5 (or perhaps even fewer) activities in one consent using broader terms such as "fundraising" "invitations to events" and "hearing from us about our other activities", with examples (e.g. inviting you to events, sending you information about our exhibitions, creating a profile of your preferences and your capacity to give) which are then described in much more detail in a linked privacy policy which is clearly signposted (e.g. hyperlinked).

Example

I am happy for my personal data to be processed for the following purposes:

❑To send me communications about the charity's events and activities (including fundraising.)

❑To share my details with [trading company].

❑To share my details with [specify other arts organisations, by name, with which you may share data]

I am happy to receive communications about the charity's events and activities (including fundraising) by:

❑Phone

❑Email

❑Post

To find out more please see our Privacy Policy which can be found [here].

How long does consent last?

Consent does not last forever. The Fundraising Regulator's guidance suggests that consent is "refreshed" at least every 24 months. 24 months is not a legal requirement – GDPR does not set a specific time period. There may be good reasons for refreshing consent less frequently – for example, a venue may have supporters who historically only attend when the venue is hosting a particular kind of event, which it does every five years. In this case, the venue may be justified in contacting those supporters only when these events come around, and refreshing consent then, rather than in the interim.

You should have a clear policy setting out your approach to refreshing consent. If you wish to use a longer period than that recommended by the regulator, you should ensure that you have a clear justification for why it is necessary for your organisation to process the personal data for this period.

When is consent needed and are there alternative bases for processing?

Consent is one of several possible conditions for lawful processing. The other condition most relevant to arts and cultural organisations' fundraising is known as the **legitimate interests** condition, which is a three step test:

Legitimate Interests:

1. You have identified a legitimate interest for the activity in question (fundraising can be a legitimate interest).
2. The use of the personal data is reasonably necessary to pursue that interest.
3. The use is not likely to prejudice the legitimate interests or rights and freedoms of the individual data subject – i.e. you have balanced your interest against that of the individual, and the activity does not have an intrusive or negative impact which outweighs your interest.

Where this condition is being relied upon, the test will need to be documented, and the fact that this is relied upon must be included in your Privacy Policy.

Where you wish to send fundraising communications by electronic means to individuals, consent is obligatory and legitimate interests will not be sufficient. The only exceptions are situations where the soft opt in applies (see page 17) and some cases when you send it to businesses.

In summary:

Channel	Is consent needed?
POST	NO (UNLESS YOU HAVE GIVEN THE OPPORTUNITY TO OPT-IN TO MARKETING BY POST AND IT WAS NOT TAKEN)
E-MAIL	YES
TELEPHONE	ONLY IF INDIVIDUAL SUBSCRIBED TO THE TELEPHONE PREFERENCE SERVICE OR THE CALL IS AUTOMATED
TEXT	YES
SOCIAL MEDIA	YES IN SOME CIRCUMSTANCES

There are some limited circumstances in which organisations can send electronic direct marketing without consent. This exemption is known as the "soft opt-in" and is explored further on page 17. It is important to note that this exemption may only be relied upon in order where the marketing relates to products or services. It cannot be relied upon to send fundraising messages by electronic means.

Another condition that organisations may satisfy is where it is necessary to process the information for the **performance of a contract**. This would include processing data to sell tickets or products from your shop, but this condition *would not* allow you to also use that data for marketing/ fundraising – this is a separate activity and you would need to rely on consent or legitimate interests, depending on the channel used.

B: Wealth Screening

Wealth Screening/ Profiling

'Wealth screening' or 'supporter profiling' is the process of analysing data about an individual in order to tailor fundraising approaches to be more efficient and effective. If undertaking such activities, **transparency is crucial**.

The practice known as "wealth screening" or "wealth profiling" is the process of analysing data about an individual in order to estimate their potential capacity to give. In other words, it is a means of identifying and researching potential donors (including major donors) to ensure a more targeted and proportionate approach can be taken to fundraising. In the arts and cultural sector, there are two primary strands:

1. building a profile on a prospective (or existing) major donor (e.g. using information from public registers to ascertain their directorships, or information from press reports about their level of wealth and their interests); and

2. running supporter data files against other data sets which contain financial indicators, such as postcode data or information on the electoral roll – for example to try to identify possible major donors from amongst existing supporters.

both of which come under the umbrella term "wealth screening".

Organisations may undertake their own research (more typically in relation to the first process described above) or may commission a third party company to conduct such an analysis on their behalf (more typically in relation to the second process).

These practices have come under scrutiny from the ICO recently and were a feature of two monetary penalties given to large charities in December 2016, followed by 11 more in 2017. In many of those cases a key issue was that individuals were not aware this was happening. A clear, transparent privacy notice would have helped make them aware (see the examples below). Done correctly, major donor research can enhance an organisation's relationships with its supporters, allow more tailored/ targeted and proportionate fundraising campaigns, and make best use of limited or charitable funds.

Fair processing

If you are wealth screening you need to be very clear about this in privacy notices.

Transparency is crucial. The ICO has taken the view that wealth screening is the kind of processing that individuals are highly unlikely to expect as a result of their charitable giving, and so you need to inform them very clearly that you will do it so that it is then reasonably expected. The ICO's enforcement notice against one charity for wealth screening activities said that *"supporters have not been provided with sufficient information to enable them to understand what would be done with their personal data in terms of screening and thereby to enable them to make informed decisions on whether or not they wished to object to such processing"*.

If you undertake wealth screening, the wording in your privacy notice should be clear and detailed enough to give those individuals an understanding of what processes you will undertake. For example:

We will wealth screen your personal data.	This is a bad example as many individuals will not understand what wealth screening is.
We may use profiling and screening techniques to analyse your personal data and create a profile of your interests and preferences. In doing so we may make use of additional information about you, including where you live, your [age] [any other demographic information] and other information and measures of wealth, when it is available from external sources (such as public registers or online (including records that you have made public on social media) or the electoral roll). We may use third party suppliers to undertake these activities on our behalf. *This helps us understand a bit more about the people who support us so that we can make appropriate requests to those who may be able and willing to give more than they already do, enabling us to raise funds sooner and in a more tailored way than we otherwise would.**	This is clearer, as it: - explains that the personal data will be used to create a profile - explains that personal data that the individual did not provide will be obtained from other sources - is transparent about this including indicators of wealth, and the purposes of it - highlights that third parties may be involved in the process The notice should always be tailored depending on what it is you will do in practice; a case-by-case organisational approach will be required.

**Please note you should always take specific advice on the statement you use to describe wealth screening, as what is required will depend on the nature of the wealth screening you are carrying out.*

This should also be clearly drawn to supporters' attention in suitably prominent ways. For new supporters, this can be included in the first 'layer' of your privacy notice at the point of data collection. For existing supporters, it may be necessary to send them a dedicated communication alerting them to your revised policy and summarising for them the key elements involved in wealth screening, where you had not previously informed them of this (which might be one of a few key updates to your policy that you are identifying to them).

Is consent needed for this activity?

Even if the processing is otherwise fair and transparent, and the individual has been provided with the Privacy Information above, it still needs to be justified on a legal basis. There is uncertainty and disagreement over whether consent is necessary to carry out wealth screening, or whether an organisation can rely on its **legitimate interest**.

The ICO takes the view that *some* wealth screening activities, such as segmenting your database by reference to postcodes or other information you already have can be justified under the legitimate interest condition (and does not therefore require consent). However, *"far more intrusive are activities such as profiling individuals, particularly where this involves getting more information that the individual has not given you, either directly or via third-party companies. In these cases the legitimate interest condition is highly unlikely to apply. So **you'd need to seek the consent of individuals before doing such processing**."*

Consent appears to be viewed by the ICO as the most relevant legal basis for wealth screening. However, it is not always a viable option, and organisations can lawfully undertake many aspects of major donor fundraising on the basis of legitimate interests. In such cases, you will need to consider

whether you can rely on the **legitimate interests** basis and balance your legitimate interests against those of the data subject whose information you will be processing. You will need to take into account whether the activity might be considered to be particularly "intrusive" and whether that individual might expect you to be processing their data in such a way. Whilst there is still a lack of clarity over when you can rely on legitimate interests, and what is considered "intrusive", a good approach may be to put yourself in the shoes of your audience and consider how they would feel about the activities you are undertaking in relation to them; taking into account factors such as how readily available the information is (for example, information obtained from a third party about the amount left on an individual's mortgage would be more intrusive than information taken from the Rich List).

Obtaining information from other sources or using third parties

Examples

A gallery compares its supporter database against the Forbes rich list to create a shorter list of individuals who may receive a targeted approach as potential major donors.

A museum uses an agent to carry out searches about its supporters from public sources. The information gathered includes an estimate of the value of the individual's house and details of their company directorships.

If you obtain personal data from public sources you should say so in your privacy notices.

Following the examples above:

- Comparison against the Forbes rich list is unlikely to be so intrusive into the individual's privacy that the processing is likely to prejudice the rights, freedoms and legitimate interests of the individual. However, this example is finely balanced and it is currently not clear if the ICO would view this as an activity which could be carried out in reliance on the "legitimate interests" condition. Similarly, segmenting your database using postcodes that you know contain wealthier individuals may not require consent, and the ICO has cited segmentation of an organisation's own database as an example of something that may represent a relatively low level of intrusion into privacy.

- Searching external public sources for information about a person's financial position (which in itself can range from, for example, the electoral roll to an individual's public posts on social media such as Facebook or LinkedIn) is more likely to be considered intrusive by the ICO and require consent.

- Where using external companies, they are likely be data processors. You will need to consider all of the above but also the added requirements that stem from sharing data with a data processor. See more information below about sharing personal data with service providers, which would include those conducting wealth screening. You can find the ICO's guidance on data controllers and data processors here.

In all of these cases, the activity should be brought clearly and prominently to the attention of the individual.

C: Compliance by fundraising channel

Below we set out the specific requirements (including whether consent is required) for fundraising in different scenarios, by reference to the channels of communication which will be most relevant to arts and cultural organisations.

In all cases, you will need to have explained that you will undertake the proposed fundraising activity as part of the Privacy Information and you will need to give the individual an opportunity to opt-out of receiving fundraising communications. Individuals can always ask data controllers to stop processing data about them for Direct Marketing purposes. If you receive such a request you should add this to a "suppression list" recording that fact and refrain from sending them further fundraising communications unless they ask you to.

It is also important that you record clearly the appropriate permissions you hold for each individual to ensure that you can demonstrate compliance.

Remember: these rules only apply to Direct Marketing. They do not apply to all communications.

Further detail on the below can be found in the ICO's Direct Marketing guidance here.

Fundraising Preference Service
The Fundraising Preference Service (**FPS**) launched in July 2017. It allows individuals to stop direct marketing communications from one or more selected charities in the UK and is operated by the Fundraising Regulator. The FPS will contact any charity subject to an opt-out request with a 28 day deadline to remove the person's details from its mailing lists. If you receive such a request, you must remove the individual from your mailing list within 28 days and not send any further Direct Marketing to that individual (via any channel).

Fundraising by post

Is consent needed? ***No***

Privacy notice

Although consent is not needed, you need to have provided the Privacy Information, so that receiving fundraising by post is consistent with an individual's expectations. If you informed them in your privacy notice (e.g. on a donation form, website sign-up page, or verbally over the telephone) that you will send them fundraising communications by post, then it will be consistent with their expectations.

If you have not been able to give them this information beforehand, or had collected their address for a different purpose (e.g. they purchase something from your shop, and your website's privacy policy did not explain that you would contact them to fundraise), you could tell them about this at the same time as sending the fundraising mail, though this is not considered best practice.

Opt-out

An individual who wishes not to receive fundraising communications by post can register with the Mailing Preference Service (**MPS**). The Fundraising Code requires you to check against the MPS before sending, as you must not send fundraising by post to MPS registered individuals unless you can evidence a prior relationship. If you have consent or have given clear Privacy Information and a prior relationship you can still contact these individuals.

Example	**Guidance**
A museum sends a regular newsletter to its members and friends which includes content which would be considered Direct Marketing, such as a call for donations for refurbishment of its building, and also content which might be Direct Marketing about its upcoming exhibitions. The museum's website clearly states that it will contact its members and friends from time to time with information about its activities.	Consent is not required to send this communication by post. Provided these individuals have received the Privacy Information at sign-up they will expect to receive this form of communication. Because the communication contains Direct Marketing you should inform people in the communication how they can easily opt out from receiving future Direct Marketing, e.g. by sending an email or calling a number.
James purchased a mug from the museum's shop. When completing his purchase he was offered the choice of opting-in to receiving further information by post, email or SMS. James ticked the box for email and for SMS but not the box for post.	Whilst consent is not required, James has indicated that he does not want to receive further information from the museum by post. The museum should not therefore send its postal marketing to James, and its database should reflect his preference not to receive Direct Marketing by post.

Telephone fundraising (not including text fundraising)

Is consent needed?

Only if the number is registered with the Telephone Preference Service (TPS) or in the case of a business, the Corporate Telephone Preference Service. You should screen numbers against the TPS before making fundraising calls (www.tpsonline.org.uk), unless you know an individual has consented to receiving Direct Marketing calls from you.

The TPS is an established and widely known model for blocking unsolicited calls. For this reason, whilst consent is not needed to call those who are not TPS-registered, many organisations choose to obtain consent for telephone calls (as they would for emails) because consent will override TPS registration.

Privacy notice

As with post, you need to inform them that you will contact them from time to time to fundraise.

Opt-out

As with post, you should record the information you have given them about how you will contact them (i.e. record that they have been provided with the Privacy Information). You should also record if they have given you consent to contact them by telephone, as this will override TPS registration. Record on your suppression list if they opt out or if they register with the TPS (where you do not have consent).

Examples	**Guidance**
Sophie is making a fundraising call to an individual whose number she has because they recently bought a ticket for an event.	Sophie can make the call as long as (a) she screens the number against the TPS beforehand, and (b) the individual has been given the Privacy Information (i.e. they were informed when they bought their ticket that they may be contacted from time to time to fundraise).
Sophie is now calling supporters from the theatre's database to let them know that the theatre is being renovated and explain the ways in which they can provide support. Sophie is checking the database against the TPS. Roy has told the theatre he is happy to receive calls from them. His number is registered with the TPS. Sylvia's number is also registered with the TPS. She is a supporter but has never given consent, explicit or otherwise, to receive calls.	Sophie can definitely call Roy despite his TPS registration as he has given consent to receive calls from the theatre, which overrides the TPS. Sylvia's TPS registration acts as an objection to receiving calls. Sophie cannot call her as she has given no overriding consent.

Automated calls

The rules around automated calls (those that are made by an automated dialling system which play a recorded message) are stricter and specifically require consent.

Fundraising by email or text

Is consent needed? ***Yes***

These are both forms of electronic marketing, so consent is required before making the fundraising approach. This is the case even if there is another purpose for the email, but it includes Direct Marketing such as a request for a donation. For example, if a venue sends an email confirming a booking which also asks for a donation.

As explained above, consent means taking a positive action on an informed basis (such as ticking a box). The ICO's guidance on Direct Marketing states that *"consent for electronic marketing messages is more tightly defined than in other contexts, and must be extremely clear and specific"*.

Note the Audience Agency's guidance generally on what consent needs to be obtained, and what should be included in the privacy notice, where data sharing with a view to sending electronic direct marketing is anticipated: https://www.audiencedatasharing.org/guidance.

Two exceptions to the consent requirement which may be relevant for arts and cultural organisations:

The soft opt-in (1)

PECR provides a limited exception to the requirement for consent for electronic messages in the context of individuals purchasing a product or service. This can be relied on where:

- the contact details of the individual were collected in the course of a sale of a product or service – this includes details obtained during 'negotiations' for a purchase (for example in responding to a quote, but not to just clicking on a website) (*Note this will not include situations in which a person's details were collected when they made a donation to the organisation*);

- the sender only sends marketing material relating to their own similar products and services; and

- when the address was collected, the opportunity to opt-out of receiving marketing communications was offered and not taken. The opportunity to opt-out must be given to the individual with every subsequent message.

This exemption is narrowly defined and only applies to commercial marketing so it would not allow you to send appeals or requests for donations even where an individual has donated to you previously.

Examples	Guidance
An individual buys a book from a theatre's online shop. The shop is operated by the theatre's trading company.	The trading company can send the individual emails about new ranges in the online (or physical) shop, provided it always offers the opportunity to opt-out. It cannot send information about shows at the theatre as it does not operate those – they are provided by the theatre directly. Similarly the theatre cannot send fundraising email appeals to this individual since it will not have obtained their consent.
An individual buys tickets to see a show at the theatre.	As explained above, the shows are put on by the theatre directly. The theatre could email the individual about upcoming similar events it is hosting, but not about the products in its trading company's online or physical shop. The soft opt in exemption will not permit the theatre to send fundraising appeals by email to this individual since it will not have their consent to do so.

Business to business marketing (2)

The PECR consent rules apply to individuals only. They do not apply to 'corporate subscribers' – i.e. businesses which have corporate identity (not including sole traders or individual consultants). It should be a genuine business to business marketing purpose (for example promoting your corporate event hire) and not simply a 'workaround' - marketing to the individual but via their business address.

Privacy notice

Privacy Information must still be given in the form of a privacy notice or otherwise (even if the soft opt-in applies).

Opt out

Emails and texts should provide clear instructions for unsubscribing from future emails of that kind (e.g. via an "unsubscribe" link at the bottom of an email, or by offering an opt-out via text such as "text STOP to 12345"). Even if the soft opt-in applies, and even where the email is business to business the individual must still be provided with the opportunity to opt-out (and in this case in **each subsequent email or SMS**) – unless it is to a generic email address which does not contain personal data (e.g. a name) – for example admin@corporate.com.

You should update your database to record that you have an individual's consent and you should record if they opt out or register with the TPS.

Social media

Is consent needed? ***Yes, for direct messages***

With the emergence of online messaging platforms (such as “WhatsApp”) and their increasing use as a substitute for “traditional” SMS and email, it is likely that in the next few years online messaging will be subject to specific regulation. However, for the time being, marketing messages sent directly through platforms such as Twitter, Facebook or LinkedIn are likely to be treated the same as more traditional “electronic messages” like text and email.

The position with advertising through social media other than sending direct messages, for example using custom audience tools, is less clear. In the light of the Cambridge Analytica scandal, extra care should be taken with the use of social media particularly where you may be obtaining more information that the individual did not provide to your organisation directly.

Examples	**Guidance**
You upload your database to Facebook or Twitter to make use of their “Custom Audience” tools – they will match the data with their own user profiles and display your marketing material to them on their social media feed.	Custom audience tools work by matching information you provide to information held by the social media site. Where a match is made, advertising can be sent through the site. Although it may not be immediately obvious, and the position is not entirely clear, electronic advertisements sent in this way may constitute "electronic mail" under PECR in which case consent may be required. Depending on which Facebook tools you plan to use to fundraise, it may be appropriate to seek advice on whether individuals’ consent is needed.
You pay Twitter to promote a tweet, which is not targeted at particular Twitter users.	Provided promoted tweets are not being targeted to individuals, this is less likely to be treated as “electronic mail” and therefore less likely to require consent.
You message an individual directly and personally on LinkedIn inviting them to a fundraising event.	This is an electronic marketing message subject to PECR and you would need consent and to have provided the Privacy Information.

Face-to-face Fundraising

Everybody in your organisation should be an advocate, from curators to front-of-house staff, trustees to volunteers. They should all be aware of the data protection and other legal requirements of such activity, including face to face fundraising.

There are detailed rules which apply to public charitable collections and "commercial participator" and "professional fundraiser" arrangements, which are summarised, briefly, below. However, arts and cultural organisations are more likely to be fundraising on their own private premises e.g. in the museum, gallery or shop. This is not public, or "door to door/ street" fundraising, so those detailed rules will not apply, nor will the rules on electronic Direct Marketing, as you will not be marketing via the relevant channels (email, SMS, telephone etc.).

Examples
A volunteer takes people on a tour of your institution. At the end, they explain that the organisation is a registered charity, that it is undertaking renovations, and that their support would be appreciated – they can either donate or can sign up as members if they would like but are not obligated to.
Sir Henry Huit offers to host a fundraising reception at his private estate. You organise the event. Invitations are sent to those on your database (by email – they have given consent). Your director makes a speech thanking all for their generosity and the event is an opportunity to approach them to discuss ways in which they could support the organisation.

In both examples the regulations which apply to public fundraising will not be triggered - you either do not require permission to undertake the activity on the premises, or you have the express permission of the private property owner. However, what is considered to be a "public place" is not defined in the relevant law and could include a place which is technically private property but where members of the public go – for example shopping centres and supermarket car parks. Therefore, when carrying out fundraising at a potentially public location, specific advice should be obtained.

There is a possibility that in the example of Sir Huit above, if the event were open to the public rather than individuals invited either by him or by the organisation, it might be considered to be taking place in a "public place", although again this would depend on whether individuals need tickets to gain entry.

The individuals donating at the above private events may simply donate via a collection box (in which case you will not receive their personal data so data protection rules will not be relevant), or may donate online, sign a donation form or sign up as a member, in which case you will be processing their data and they should receive Privacy Information in respect of the information they are providing and have the opportunity to consent before you send them further fundraising communications.

Private site fundraising rules

There is always a need to fundraise responsibly, given the media's interest in and focus on charity fundraising practices and the resulting enhanced risk of harm to your organisation's reputation. The Fundraising Regulator has published a rulebook on private site fundraising which can be found here - https://www.fundraisingregulator.org.uk/2017/08/09/regulator-releases-new-rulebook-private-site-fundraisers/.

The **key rules** from the Fundraising Regulator's Private Site Rulebook are that fundraisers:
- Must act responsibly, i.e. not in a way that might cause members of the public to become anxious, and not in a way that may bring the organisation into disrepute (e.g. smoking or drinking, lewd behaviour and swearing, exerting undue pressure on members of the public to donate).
- Must not act dishonestly or manipulatively.
- Must not sign up any person at any time who they may have reasonable grounds for believing are in vulnerable circumstances so may not be able to make an informed decision to donate.
- Must not sign up any person under 18.
- Must make a legally compliant statement that they are fundraising on behalf of X charity, and that they are being paid (unless they are volunteers).
- Adhere to the '3 step' rule – not take more than 3 steps alongside or in pursuance of a member of the public, and not deliberately obstruct.
- Not work outside the confines of the private site.
- If obtaining consent to future contact, must clearly explain that members of the public can choose to give or withhold that consent, and ensure they understand what is being agreed to.
- Not engage an individual who has clearly indicated they do not wish to be engaged.
- Must have a clearly displayed ID.

Public (street) collections

This will not apply to fundraising on private charity property – for example, to employees who fundraise as part of their role in a gallery or box office. Engaging in public street collections is not a very common method of fundraising employed by arts and cultural organisations.

In England and Wales these are governed by a patchwork of historic legislation. More information can be found at the Institute of Fundraising's website here. In summary:

- There are currently no specific regulations covering static collection boxes, but there is Fundraising Regulator guidance which incorporates applicable principles of charity law, e.g. that boxes should include the charity's name and must include a statement that they are a registered charity: https://www.fundraisingregulator.org.uk/17-0-static-collections/. The biggest risk of conducting street fundraising is to reputation if they are not conducted in a sensible and appropriate manner (e.g. if people are harassed).

- A public charitable collection is the collection of money for charitable purposes in a public place (note above that this can cover more scenarios).

- Permission from the local authority is required and local authorities can impose fines if a person is in contravention.

- Collectors must be aged over 16 and cannot be paid (though paid employees acting as collectors can do so as long as they make a statement that they are being paid (though they do not need to specify how much), and must remain stationary.

The Fundraising Regulator's Rulebooks for Face-to-Face Fundraising (which cover street and door-to-door fundraising) can be found here.

Commercial Participators and Professional Fundraisers

Commercial Participator

A commercial participator is someone who encourages purchases of goods or services on the grounds that some of the proceeds will go to a charitable institution, or that a donation will be made to a charitable institution. For example, a shop selling teabags and donating a portion of its proceeds to a local museum (perhaps a museum based at the birthplace of "Earl Grey"), or a business operating a "charity of the year" arrangement.

A charity's trading subsidiary is typically not a commercial participator provided they are controlled by the charity, so does not need to comply with their regulation under the Charities Acts.

There are two main consequences of engaging a commercial participator:

1. There must be a written agreement which meets certain minimum legal requirements (including how the commercial participator will protect vulnerable people from unreasonable intrusion on their privacy and undue pressure to donate).

2. The commercial participator must make certain transparency statements at the point of sale (broadly, the amount of the price paid for each product or service which will be given to the charity (as a percentage or precise amount), the actual overall amount intended to be given by the commercial participator to the charity, and if that amount is not known, an accurate estimate.

These obligations fall directly on the commercial participator but the Fundraising Regulator (and the Charity Commission) expects organisations to be accountable and ensure that their agents are fully compliant with the law.

For further information see the relevant section of the Fundraising Regulator's Code of Fundraising Practice here.

Third Party Professional Fundraisers

The Charities Acts also regulate fundraising by paid, third party fundraisers – these provisions do not apply to trading companies, or trustees, employees and volunteers of the charity. It is common practice for charities to engage third party agencies to fundraise on their behalf. A professional fundraiser is a person or organisation whose main business is to raise funds for charities.

A professional fundraiser must:

1. enter into a written agreement with the charity;

2. make a solicitation statement whenever it solicits money or other property for the benefit of one or more charities;

3. make records relating to the professional fundraiser agreement available to the charity; and

4. safeguard the money they raise and pay it over to the charity promptly.

For further information see the Charity Commission's guidance on working with companies and professional fundraisers here.

D: Other Fundraising Issues

What about when we share personal data with fundraising service providers?

Many arts and cultural organisations transfer their data (or copies of it) to other organisations to provide fundraising services or outsourced elements of their fundraising (such as wealth screening as explained above) to agents providing services such as professional fundraisers, fulfilment houses or payment processing providers. Another common example is where arts and cultural organisations use cloud computing service providers. Where data is shared in this way, the charity is the data controller of the information being shared and the third party service provider is likely to be the data processor. As a data controller, an arts and cultural organisation will be responsible for everything that the data processor does with the personal data and will be primarily liable if the data processor breaches the GDPR in relation to the personal data that it is processing.

It is a legal requirement under the GDPR that where an organisation uses a data processor to process personal data on its behalf, it must have a written agreement in place with that data processor under which the data processor may only process data in accordance with instructions from the data controller, and that written agreement must contain the following minimum provisions.

That the processor will:
- only use personal data on your documented instructions.
- not transfer the personal data to a country outside the European Economic Area without your approval and putting in place certain safeguards.
- observe the confidentiality of personal data you send to them and make sure that people working on its behalf also do so.
- have in place appropriate data security measures.
- not sub-contract the work without your written permission (and where they do subcontract, do so using an equivalent written agreement, and remain responsible for the actions of the sub-contractor).
- assist you with facilitating individuals' rights data security and breach notifications; and with any data protection impact assessments or any consultations with the ICO.
- when the contract ends, either delete or return all personal data to you.
- make available to you all information necessary to demonstrate compliance (for example, by allowing you a right of audit).

In selecting third party providers, arts and cultural organisations are required to select only organisations which provide a sufficient degree of security to protect personal data.

What do we do if we have collected information improperly? Can we unlock/ use it?

You may well hold historic personal data that was not collected in accordance with the law or with the standards now imposed by the ICO.

There is no entirely safe way to unlock this data so that you can use it for fundraising. The ICO's Direct Marketing guidance states:

> *"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 as other marketing texts and emails. And calls asking for consent are subject to the same rules as other marketing calls."*

However, consent is not required to send individuals fundraising communications by post, but seeking consent this way takes the risk of assuming that the individual has not specifically opted-out of receiving marketing from your organisation.

The risk of contacting individuals who might not wish to be contacted (as your records are incomplete and you cannot be certain), is that they make a complaint to the ICO, or you subsequently become the subject of an ICO investigation for some other reason and the ICO then investigates your broader practices, and you are found to be in breach of the GDPR. To reduce this risk, where you have an existing relationship (members, customers etc.) with the individuals, the risk of complaint is likely to be lower as they may be sympathetic to your aims and activities and reasonably expect to hear from you about how they can help.

Equally, contacting individuals with Privacy Information and/ or seeking consent in relation to historic wealth screening data, where those activities were undertaken in breach of the GDPR or the Data Protection Act 1998 will always carry a risk – there is no guaranteed way of unlocking this data without taking a risk that an individual will complain to the ICO about the historical breach that has taken place. We therefore suggest that serious consideration is given to the value and usefulness of such data before any attempt to "unlock" it is made. Where you decide to contact individuals whose details have been wealth screened in breach of data protection law we recommend that specific legal advice is obtained on the approach and the contents of any communication that you plan to send.

Can we use a pre-ticked donation box?

For online purchases, organisations will often include a pre-ticked box to represent that the individual agrees to top up their purchase (of, for example, a ticket to an event, or an item from an online shop) with an additional donation to the venue.

Pre-ticked boxes automatically adding on a donation may not comply with consumer protection law. If the customer is to be charged any extras (including donations), the customer should give their consent to making those payments on an opt-in basis.

E: Further Information and Resources

Other GDPR compliance requirements

This guide only covers those aspects of GDPR directly relevant to your fundraising practices. However, any breach of the GDPR has the potential to harm your relationship with supporters. We suggest you read the ICO's guide to the GDPR which can be found here - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/. Some of the key things you should be doing include:

- considering whether your organisation needs to appoint a Data Protection Officer;
- reviewing your existing privacy policies and notices;
- reviewing your existing data processing and data sharing agreements;
- audit and document the personal data you hold and use, recording where it came from and who it is shared with;
- developing a data breach response plan – the GDPR will require organisations to notify the ICO of all data breaches without undue delay and within 72 hours unless they are unlikely to result in a risk to individuals; and
- putting in place measures for accommodating individuals' privacy rights – including the new 'right to be forgotten' where it applies.

On the horizon

The new E-Privacy Regulation

Whilst PECR is the current UK law relating to electronic communications (i.e. essentially as an anti-spam measure), electronic communications regulation is currently being reviewed at an EU level and it is expected that a new E-Privacy Regulation will apply in the next 12-18 months. This is likely to include:

- Requirements for consent for electronic direct marketing
- Regulation of cookies and similar technologies

Other useful resources

ICO website – the UK's data protection regulator - www.ico.gov.uk

The Audience Agency – an organisation which has published guidance for Arts Council England on data sharing - https://www.audiencedatasharing.org/

Fundraising Regulator – the regulator of fundraising practices in the UK - www.fundraisingregulator.org.uk

Institute of Fundraising – the professional membership body for UK fundraising - www.institute-of-fundraising.org.uk/home/

Direct Marketing Association – a voluntary membership body for direct marketing best practice - www.dma.org.uk/

Charity Commission guidance for trustees on charity fundraising: www.gov.uk/government/publications/charities-and-fundraising-cc20/charities-and-fundraising

Checklist – Key Points

- Individuals whose personal data you process must be given information about who you are and what you will do with their personal data. This is usually given at the point of collection in a privacy notice.

- Under the GDPR, more information will need to be provided in a privacy notice.

- Fundraising communications are Direct Marketing. You will need the consent of the individual to send them:

    - if they are sent via email, SMS, automated call or online messaging; and

    - if they are made via telephone to somebody registered with the TPS.

- You do not need consent to send individuals fundraising communications by post.

- In all cases individuals can opt-out, and if they do so you should record their opt-out on a "suppression list" to ensure they are not inadvertently sent communications they have not consented to. Individuals can opt-out directly, or via the FPS.

- Wealth screening/ profiling covers a range of activities which the ICO believes require consent in all but the least-intrusive cases (such as using data you already have to segment a database by reference to postcodes). In all cases you need to inform individuals clearly that you will be doing this, by providing as much information as possible. In some cases legitimate interests can be relied upon, provided the activity is not too intrusive, and the balancing exercise is carried out and clearly recorded.

- When engaging others to process data on your behalf, you must have a written agreement in place with them. Under the GDPR, you are primarily responsible for their breaches of data protection law.

- There is no risk-free way to "unlock" data that was collected improperly or which you are unsure about. The best way to avoid being in this situation is to have clear privacy notices and to obtain the correct permissions at the beginning of your relationship with each supporter.

- It may not be advisable to use a pre-ticked box to add donations on to a purchase on your website.

Further things you may consider, for best practice and to ensure compliance, are:

- Putting in place appropriate internal policies on data protection compliance, and on data retention.

- Reviewing the privacy policy on your websites.

- Training all staff on data protection and fundraising compliance.

Key terms defined

Data controller:	An individual or an organisation which, either alone or jointly with others, directs how and why personal data is to be processed. The data controller will be ultimately responsible for compliance with the GDPR.
Data processor:	Any person (other than an employee of the data controller) who processes data on behalf of and at the direction of the data controller. For example volunteers and consultants.
Personal data:	Data that relates to a living individual who can be identified either directly from that data or from that data combined with other information. This includes a person's name, address, email address etc. and can in some circumstances extend to their computer IP address.
Processing:	Defined very widely to include obtaining, recording, organising, using, disclosing, deleting and even simply holding data. Most things your organisation does with personal data will amount to processing.
Sensitive personal data:	Personal data which relates to an individual's: - political opinions; - racial or ethnic origins; - religious or philosophical beliefs; - trade union membership; - mental or physical health; - biometric data for the purpose of uniquely identifying them; - genetic data; - sexual life or orientation; or - criminal record (including any allegation of the commission of an offence) This final category is not strictly sensitive personal data but is also subject to additional protections.