YOUR HOSPICE LOTTERY AND MAKE A SMILE LOTTERY CODE OF CONDUCT AND COMPLIANCE 2025

This conduct and compliance document includes essential safety measures that have been implemented to protect our team and the public. Every fundraiser must read and sign this documentation as well as being given Gambling Commission Training before being allowed to represent the hospices and charities we fundraise for.

- ✓ Every fundraiser must have had a valid DBS check before starting work.
- ✓ All fundraisers will always have identification on them.
- ✓ Pictures of all fundraisers will be evident on the Your Hospice Lottery and Make a Smile Lottery websites.
- ✓ The Fundraiser Procedure is in line with some of government and governing bodies' recommendations.
- ✓ Fundraising tablets are powered by Ideal Host which includes a social distancing function in which the potential lottery player can choose to confirm their play on their own device so they will not need to touch the screen. Fundraisers will use anti-bacterial wipes to ensure devices are clean.

FACE TO FACE FUNDRAISING PROCEDURE

Public Lottery Fundraising

This guidance is part of a series of resources produced by the Fundraising Regulator and Chartered Institute of Fundraising that aims to support charities and other fundraising organisations to be able to return to fundraising activities in a responsible way.

Fundraising in public: principles and key considerations

Fundraising must be carried out responsibly and the health, safety and wellbeing of the public, fundraisers and volunteers must come first. The risks associated with the activities are being regularly monitored and managed.

Give way to the public.

Our Fundraisers will never cause any physical obstruction to the public. If any setting does not enable the fundraiser to give way to the public and maintain social distancing throughout then fundraising will not take place in that setting.

Maintain a static position.

The code allows fundraisers to approach the public, for example by taking steps alongside them.

Make sure your behaviour is respectful.

You should expect that at this time some members of the public may be more anxious than usual about interacting with others. Check that an individual is happy to talk with you and be respectful about personal space while maintaining one metre distance. You should be mindful of how your interaction can affect others in a public space, so it's important to be aware of others around you and the space you are in.

Use fundraising sites responsibly.

If part of a site becomes particularly crowded, for example, due to multiple queues forming, you should reposition yourself while also meeting the requirements of any Site Management Agreement that may be in place.

Limit the number of fundraisers.

- For door-to-door fundraising, no more than four fundraisers will work together at the same time and only one fundraiser at a time will approach a household.
- For private site fundraising, the number of fundraisers will be set by the terms of the relevant agreement with the site owner.

Make sure ID badges and mandatory information is accessible.

Lottery Fundraisers will always have identification badges on them. Lottery Fundraiser pictures are also apparent on the Your Hospice and Make a Smile Lottery websites

Carefully select your door-to-door fundraising territory.

When selecting territories in which to fundraise, be particularly mindful of places where there may be greater numbers of people who may be more vulnerable. Keep a knock sheet and record every door that has been approached.

Co-operate effectively with third parties.

If you work with third parties, it is important that you are clear about your expectations in relation to fundraising conduct and the approach that should be taken as pandemic restriction measures are eased. All agencies that work for MAS and YHL will provide copies of their risk assessment and policies.

Listen to feedback.

We listen and reflect on feedback we receive from the public, staff, and volunteers as this will help to inform the way we carry out fundraising during this period. Activity will be continually reviewed, considering comments, complaints, and feedback.

Consider the needs of people in vulnerable circumstances or with protected characteristics.

It is inevitable that fundraisers will meet people who may be in a vulnerable circumstance or need additional support to make an informed decision. You must take into account the needs of anyone who may be in vulnerable circumstances.
You should also consider the needs of those with protected characteristics, such as those who are hearing or visually impaired.
Please also refer to our vulnerable people policy on how to interact with vulnerable persons.

Do not apply undue pressure to donors.

Be polite and respectful.

Be mindful of how the public may respond to your fundraising.

Do not knock on doors with no-canvassing stickers/signs displayed.

Vulnerable People Guidelines

It is inevitable that you will come into contact with people who may be in a vulnerable circumstance or need additional support to make an informed decision. This guidance is intended to help and support you deal with those situations.

It is important to proceed with caution with any members of the public who you suspect may be vulnerable. We must do our best to avoid signing these people up even if they have indicated that they wish to do so! But equally we must not be seen to be discriminatory or judgmental of potentially vulnerable members of the public. These guidelines will assist you in deciding whether the individual with whom you are speaking could potentially be vulnerable and therefore you should end that interaction and you shouldn't sign them up.

"Vulnerable" is defined as somebody who you suspect may not be capable of informed consent about what they are doing - i.e.: they don't completely understand what they are signing up to do or what happens next. The most common types of vulnerability in this context are:

- Physical and mental medical conditions, disabilities, and difficulties (both permanent and temporary, including learning difficulties)
- Age
- Stress and anxiety
- Poor grasp of English
- Under the influence of alcohol or drugs.

If you believe that an individual may be in a vulnerable circumstance or unable to make an informed decision, then you should end that interaction.

How you can identify someone who may be vulnerable;

- Asking irrelevant and unrelated questions.
- Responding in an irrational way to simple questions.
- Asking for information to be continually repeated or continually asking the same questions.
- Obviously not understanding what you are saying and changing the subject of what you are discussing
- Taking a long time or displaying difficulty in responding to simple questions or requests for information.
- Displaying signs of forgetfulness.
- Indicating that they are currently stressed or in difficult times (e.g.: because of job loss, bereavement, ill child or parent, having to act as a carer for a child, parent or relation)
- Indicating lack of affordability to maintain the donation for any of the same reasons
- Giving a statement such as 'I don't usually do things like this, my husband/wife/son/daughter takes care of it for me'.
- Saying that they are not feeling well or not in the mood to continue.
- Indicating in any way that they are feeling rushed, flustered, or stressed
- Unable to read or understand the information you are giving to them
- Displaying signs of ill-health such as breathlessness or looking exasperated or discontented.
- Indicating that they are not financially capable of making and maintaining the donation, e.g.: they say that they never have any spare money and can barely afford to pay their bills or rent, they are in debt, they take lots of loans

Age does not necessarily mean that an elderly person is vulnerable. But please be aware of the above indicators when engaging with an elderly person in order to judge whether s/he is potentially vulnerable.

How you should engage with someone you suspect may be vulnerable

It is important to always clearly explain the reason you stopping and engaging with any person you speak to whilst you are fundraising. If you suspect, once your engagement with that person has started, that the person may be vulnerable then please take extra care and do the following:

- Explain as clearly as possible the reason for you stopping that person
- Ensure your ID is clearly on show (photo facing out) and hold it out for the person to see.
- Talk in clear language, avoiding words and phrases that may be hard to understand (but avoid shouting).
- Repeat information.
- Be patient and do not rush.
- Repeatedly check the person is happy to continue.
- Ask if they would like to talk to anybody else before making a decision.
- Check their understanding at relevant parts of the engagement
- Ask if there is anything that needs further explanation

How to end a conversation with someone who you feel might be vulnerable

If you believe that the person with whom you are engaging is not capable of informed consent to make and maintain the donation, then you should end that engagement. But this must be done politely and courteously.

A polite way to end the engagement is to say, “I’ve taken up enough of your time today, thanks for listening”, or “Maybe you need some more time to consider whether you’d like to support <the charity/the hospice>.”

● If the individual is keen to donate but you have identified them as a potentially vulnerable person, explain to them the direct methods to do so via the charity website and main telephone number.

● If, at any stage during or after the engagement. you suspect the person has been alarmed, distressed or confused by your conversation, contact your Manager and report the incident.

Cybersecurity Advice for End Users

Dear end users,

It is not with any pleasure that I write this to you, nor is it intended to make you feel like you've done anything wrong. You might have - you just didn't realize it, but don't worry, you're not alone. In fact, I imagine many people that you work with have fallen prey to one or more of the behaviours that I mention.

You probably believe magic goes on behind the velvet curtain labelled IT that protects your computers and mobile devices from harm, and, in a way, there is. IT staff work tirelessly to prevent all of those desktops, servers and mobile devices from getting hacked or infected with malware, ransomware, and other security threats. The truth is those desktops, servers, mobile devices, and networks are only as secure as you allow them to be.

That's right, in many instances the burden falls on your shoulders. Don't worry it's not that hard.

Instead of couching this advice in terms you may or may not understand, I'll make it as clear as possible. The best piece of cybersecurity advice I can give you is this: When in doubt, don't do it. Such generalities could leave you staring blankly at your screen and unable to function, so here are some specific security best practices.

- Don't click suspicious links. If you don't know if a link is suspicious, ask.
- Don't install any software on your PC or mobile device unless it comes from the operating system's built-in software store.
- Don't install browser add-ons unless they are sanctioned by your company.
- Don't visit websites that seem dodgy. What is a dodgy website? Products advertised on social media, sites that advertise products or services that sound too good to be true, sites that want to install applications on your computer, or any domain found on a list like the Fake Sites Database.
- If you absolutely must visit a dodgy site (say you're doing research for a marketing department and want to know why a product is listed as must have), do it on a tablet that can easily be reset to factory default and doesn't contain company data.
- Update your passwords with really strong ones that you can't memorize. I know that's a pain, but there's a solution: Ask your IT staff about how to use a password manager.

- Don't open email attachments that haven't been checked by your antivirus package.
- Don't open text messages from unknown senders.

I know this list seems daunting, but it all supports the original idea of, "When in doubt, don't do it."

It is no secret that, among IT professionals, the pervading feeling is that the weakest link in a company's security is the end users, but it doesn't have to be that way. All you must do is stick to the above list of cybersecurity best practices, and you'll make the lives of your IT staff exponentially easier.

But don't take this personally. It's not you. Actually, it might be you. But not 100% of the time, more like 80-90%.

Just remember, it's not that hard to keep those PCs safe from evening wear and formalwear… got you again! Come on, end users... keep up with me.

You can do this. I have faith in you. But just in case, repeat to yourself, "When in doubt, don't do it."

Thanks for reading

St Helena IT Department.