



Inheritances And Tax



Hello again, and welcome to our Spring 2026 Newsletter. In this edition we will be dealing with the position of pensions in personal estates, and the effect on Inheritance Tax liability; and also we include a 'word to the wise' from our Operations Manager, Aaron, regarding scams and the safety of your data. Well worth a read!

But let's update everyone on the pension changes:

Pension Death Benefits and Inheritance Tax Changes from April 2027

We have reported previously on the upcoming changes to the treatment of an individual's pension scheme with regard to taxation within the estate – and now with less than 12 months to go before these momentous changes take place – it's time for an update.

From 6th April 2027, significant pension Inheritance Tax changes (PIT) will come into effect, fundamentally altering how unused pension funds and death benefits are treated for Inheritance Tax (IHT) purposes. These changes mean that the value of an individual's pension will be included as part of their estate value when calculating IHT.

However, to clarify a regular question that comes our way – the existing spousal exemption for benefits passing to a surviving spouse or civil partner will be maintained. The scheme would not be inherited as a tax-free sum if death occurs after the age of 75, it will be inherited as a pension scheme and taxed as income in the hands of the surviving spouse, but no IHT liability will arise at that point.

To clarify this before and after 75 rule, unused pensions BEFORE age 75 can be passed on tax-free to a spouse. This includes any remaining tax-free cash still unused in the scheme. Beneficiaries can take the funds as a tax-free lump sum; move the funds into a 'beneficiary drawdown' account; or take an annuity tax-free, provided the benefits are paid within 2 years of the scheme being notified of the death. If the pension upon death before age 75 is inherited by a spouse, they can take the full value as a tax-free lump sum; or move them into a 'successor's drawdown account'.

The reason these changes are coming into force is that the Government and HMRC were concerned that pension schemes – from 2015 and as advised by ourselves – were becoming IHT prevention schemes, and were not being used for the purpose for which they were designed, i.e. as a pension to provide income in retirement. (Spoilsports!)



Personal Representatives

It will be the responsibility of the Executor (personal representative) of a person's Will, to pay any tax due, and the scheme itself can pay the tax directly to HMRC. Pension scheme administrators will acquire new powers to allow this to happen, but the responsibility will be on the personal representatives to inform the administrators of any tax due. We would suggest when this point happens, have a conversation with us.

1. Personal representatives must identify what pension benefits the deceased had.

(Tip: – Consider consolidation of pension schemes to ensure accuracy of valuation and that no scheme is missed)

2. Personal representatives value the estate. The personal representatives gather information from the scheme(s) and other assets within the estate to determine total value and whether an IHT return needs to be made to HMRC

3. Personal representatives file the IHT notification to HMRC and pay the tax if appropriate – either directly from the estate or via the pension scheme. Note: the pension scheme can only pay the liability on itself as a pension plan; and not on the total liability of the estate. If additional IHT is due in total – on top of scheme tax – this must be paid separately.

If no IHT is due, the personal representatives can inform the pension administrator accordingly and continue to distribute the estate assets according to the Will. If IHT is due the personal representatives determine the amount due on the schemes and inform the administrators and submit an account to HMRC. (Complex) If, once the estate is finalised and completed, an overpayment of IHT has been made by the scheme, a refund can be applied for.

Let's look at an example of post April 2027 rules;

Tom's total estate is £2 million with pension assets amounting to £1 million. He dies at age 77 with no children. The pension is left to his sister Barbara.

IHT Calculation:

Estate subject to IHT: £2,000,000 less £325,000 (IHT Nil Rate Band allowance) = £1,675,000

IHT liability £1,675,000 x 40% = £670,000 (Tax Bill)

Process:

The Personal representatives pay the total charge and recoups £335,000 from Barbara.

As a result, Barbara receives £1,000,000 pension assets - minus - £335,000 (payment of IHT to the personal representatives) minus - £299,250 (Income Tax at marginal rate on pension), resulting in a net amount to Barbara of £365,750.

So we have a current situation up to April 2027 where inheritance of tax-free value can still be achieved if death occurs before Age 75.

Post April 2027

Most unused pension funds regardless of age at death will be counted as part of an individual's estate for IHT purposes. Spousal exemption will still apply for IHT purposes on death at any age, but post April 2027 benefits are taxable as Income Tax in the hands of the recipient beneficiary - even if this is a spouse.

So, start the planning process now.

Some facts

Retirement is complex - not complicated.

Plan for life - not a spreadsheet.

Time is not equal - front load retirement spending in the healthy years.

Plan for 3 spans of time:

Healthspan

Lifespan

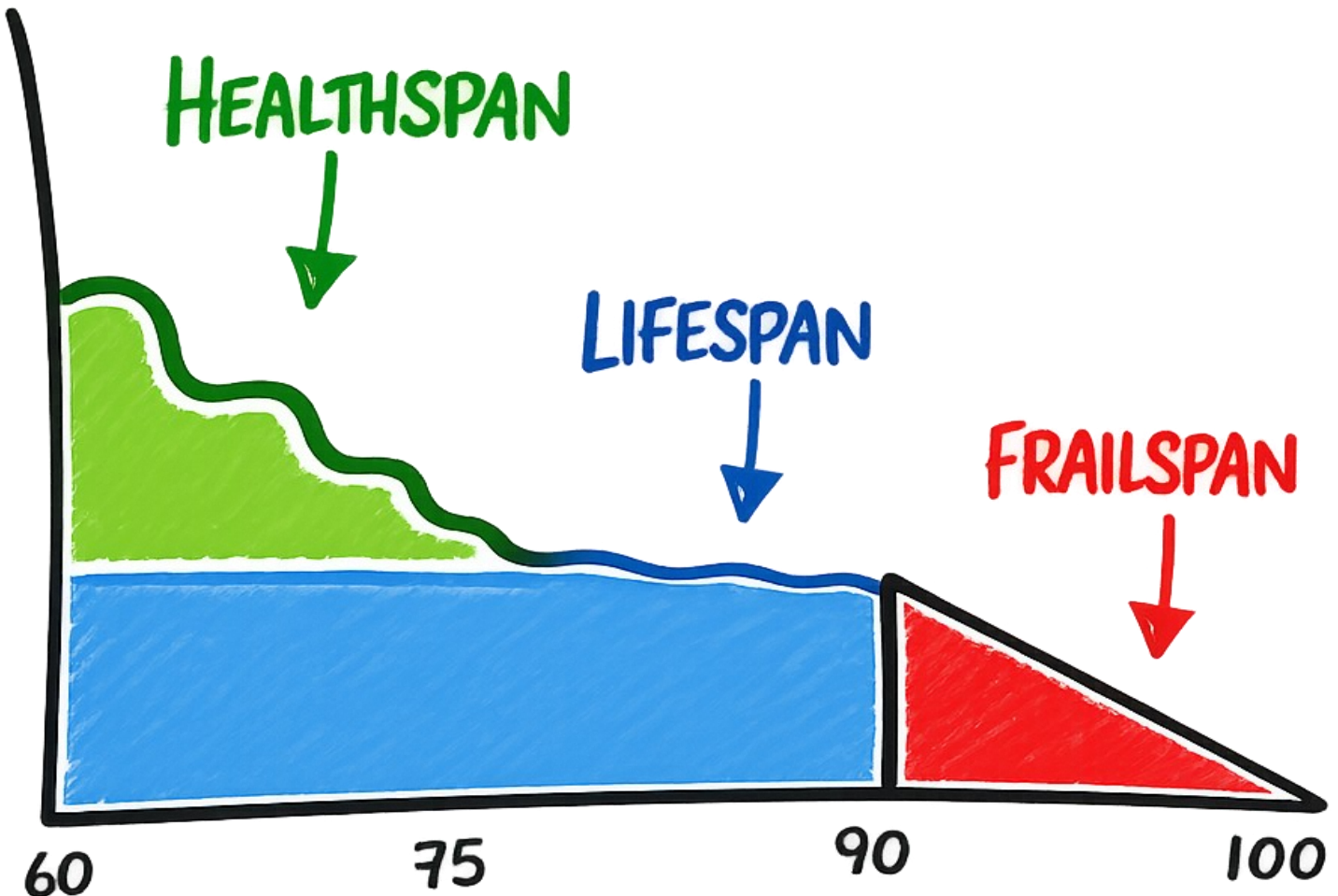
Frailspan

64% of retirees worry more about running out of money than dying!

Consider accelerating pension payments and use pensions not other assets for income. (Tax considerations)

Consider beneficiaries; you may want to gift value from your pension by taking tax-free cash allowance; or, if you want to retain control of the capital consider re-investment into Business Relief Scheme to create IHT exempt assets.

We can discuss all the above with you whenever convenient.



DATA SECURITY

PROTECTING WHAT MATTERS MOST



SECURE TODAY SAFE TOMORROW

A Note From Aaron On Data Security

Staying Safe Online: A Simple Guide to Protecting Your Money and Personal Information

We all live a bit of our lives online these days - checking bank accounts, paying bills, or reviewing investments. It's convenient, but unfortunately, it also gives scammers opportunities to try and trick us. The good news? Most scams can be avoided if you know what to look out for and take a few simple precautions.

Our job is to help you manage your finances with confidence. We provide guidance and support across a range of areas, including:

- **Investments & Pensions** – helping you plan for today and tomorrow
- **Retirement Planning** – making sure your income lasts through your retirement years

- **Financial Protection** – safeguarding you and your family from unexpected events
- **Tax Planning Advice** – helping you make the most of your money within the rules
- **Wills & Powers of Attorney** – ensuring your wishes are clear and your affairs are in order

Beyond this, we're here to support you with general financial guidance and online safety. If you're ever unsure about a message, email, or call relating to your finances - even if it's not directly connected to the services we provide - call a team member you know. We'll always do our best to help.

Our goal is simple: to give you peace of mind and the confidence to make decisions about your money safely.

Here's a friendly guide to help you stay safe.

Why it matters

Your personal information - things like your name, address, date of birth, and bank or investment details - is valuable. Scammers may try to:

- Pretend to be you (identity theft)
- Trick you into giving away passwords or PINs
- Convince you to send money to fake accounts

It sounds scary, but just being aware of the risks and keeping a few habits in mind can protect you.

The following doesn't just apply to how you deal with us, but apply generally to stay safe online.

How to stay safe

Here are some things you can do today:

1. Think before you click or reply

We'll never ask for your passwords or PINs by email or phone. If you get an unexpected message asking for personal information, pause and check it first - don't rush. Scammers often try to make you feel pressured.

2. Use strong, unique passwords

Avoid birthdays, pet names, or anything obvious. Mix

letters, numbers, and symbols, and don't reuse passwords across accounts. A password manager can help keep everything safe without having to remember them all.

3. Add extra security where you can

Many banks and online services offer multi-factor authentication. That means even if someone guesses your password, they can't get in without a second step - usually a code sent to your phone. Important: Scammers who have your email address may try to request this code themselves. They may call or message you, making it seem genuine, and ask for the code, often sent via a message to your phone. Never give your PIN or authentication code to anyone over the phone or by message. Legitimate organisations will never ask you for it.

4. Keep your devices updated

Your phone, tablet, or computer will regularly prompt you to install updates. These updates often include important security fixes, so it's best to install them when they appear.

5. Keep an eye on your accounts

Check your statements regularly and set up alerts for transactions. It's much easier to spot anything unusual early.



Red flags to watch for

Scammers are clever, but there are some common signs:

- Emails or texts pretending to be from your bank or a trusted company, asking you to click a link or provide details.
- Phone calls that claim urgent action is needed.
- Websites that look almost right but have a slightly different address.
- Pressure to act immediately - genuine organisations will give you time to think.

A few everyday tips

- Never share your password, PIN, or security codes.
- When in doubt, call us (or your bank) using a known number.
- Trust your instincts - if something feels off, it probably is.

Common Ways Scammers Try to Get Your Information

Scammers use different tricks to get your personal or financial information. Here are some common examples to be aware of:

Phishing Emails

These are emails that look like they come from a bank, utility company, or well-known organisation. They might ask you to:

- Click a link to “verify” your account
- Enter your login details or passwords
- Download an attachment that could contain a virus

Tip: Always check the sender’s email address carefully. If it looks suspicious, don’t click anything - call the company using a known number instead.



Fake Phone Calls

A scammer may call claiming to be from your bank, HMRC, or another trusted organisation. They often:

- Say there’s “suspicious activity” on your account
- Ask you to provide passwords, PINs, or security codes
- Pressure you to transfer money immediately

Tip: Genuine organisations will never ask you for your full password or PIN over the phone. If you’re unsure, hang up and call a number you know is legitimate.

Texts or WhatsApp Messages

You might receive a message that looks official and asks you to:

- Click a link to “confirm” a payment or delivery
- Provide personal details or banking information

Tip: Don’t click on links from unknown messages. Instead, go directly to the official website or call the company.

Fake Websites

Scammers can create websites that look almost identical to real ones, with minor differences in spelling or URLs. They may ask you to:

- Log in with your account details
- Enter personal or payment information

Tip: Always check the web address carefully and look for the padlock symbol in the browser before entering any sensitive information.

Unexpected Visitors or Letters

Some scammers may even try to contact you in person or by post, pretending to be a bank representative, courier, or official authority. They may:

- Ask to see documents
- Request payment or bank details

Tip: Always verify the identity of anyone who contacts you. Don’t feel pressured to act immediately - genuine organisations will give you time.

Beware of AI Scams

Artificial Intelligence (AI) is changing the way scammers operate. While AI can be very useful, it can also be misused to trick people. Some examples include:

AI-generated emails or messages that look very convincing, pretending to be your bank, a family member, or even a trusted adviser.

Fake audio or video calls (“deepfakes”) where a scammer imitates someone you know to ask for money or personal information.

Automated scam messages sent at scale, making it easier for fraudsters to target lots of people quickly.

What to do:

Always double-check the sender and don't trust urgent requests blindly.

If someone is asking for money or sensitive information, contact the person via another form of communication before taking any action. Perhaps ask a specific question only they would know the answer to.

Treat unexpected calls, messages, or videos with caution, even if they seem realistic.

AI scams are just another reason why your awareness and personal connections are your best protection.

What to Do If I Have Been Scammed?

Even the most careful people can sometimes be targeted. If you think you've been scammed, it's important to act quickly, but stay calm. Here's what to do:

1. Stop All Contact

Do not reply to any emails, texts, or calls from the scammer.

Do not click on any links or download any attachments.

2. Secure Your Accounts

Change passwords and PINs for your online banking, email, and any affected accounts.

Enable multi-factor authentication if possible.

3. Report It

Call your bank or investment provider immediately to stop any transactions and seek advice.

Report the scam to official authorities:

The Police

Your bank or financial provider's fraud team

4. Document Everything

Keep emails, messages, and any other correspondence from the scammer.

Note dates, times, and amounts involved - this can help investigators.

5. Learn and Protect Yourself

Review how the scam happened and take steps to avoid it in the future: strong passwords, cautious clicks, verifying messages, and staying alert to AI or phishing scams.

Remember: being scammed isn't a sign of failure - it can happen to anyone. Acting quickly and using the support available is the best way to minimise any impact.

Summary

Online banking and managing your finances can be simple and convenient - but it's important to stay alert. Scammers use emails, phone calls, messages, and fake websites to try and steal information, so a little caution goes a long way.

By following a few simple habits - thinking before you click, using strong passwords, enabling extra security, keeping devices updated, and monitoring accounts - you can protect yourself and your money.

Remember, many of you know our team very well, and we want to reassure you: if in doubt, pick up the phone and call a team member you know. Even if you just want general advice about staying safe online - not linked to the services we provide - we'll always do our best to help. That personal connection is one of the strongest ways to stay safe.

Stay aware, stay cautious, and don't hesitate to reach out - online safety is easier when we work together.

Disclaimer: We are not trained cybersecurity or legal experts. The information in this Newsletter is provided to help raise awareness and support safe practices online. It is general guidance only and should not be relied on as professional advice. If in doubt, please seek advice from the appropriate experts.



POINTS — FOR — REVIEW

Check Your Will

From April 2027, personal representatives (executors) become liable for reporting unused pension benefits in an estate to HMRC. Make sure your executors are aware of the new rules.

If you are divorced, check that any old Will leaving everything to a former spouse is updated. Wills have been used as guidelines to pension scheme administrators in distributing pension assets, and a former Will leaving assets to an ex-spouse - is still valid.

Nomination of Beneficiary Forms

Nomination of beneficiaries for pensions should be reviewed to ensure successful passage of pensions scheme assets to the beneficiary. If yours go directly to children - bypassing a spouse - tax could be payable on the pension scheme assets.

Remember the pre and post 75 age rule. If the pension member dies before age 75 - Income Tax does not apply. If the member dies after age 75 the benefits will be subject to Income Tax when taken. IHT assessment happens pre and post age 75 from April 2027.

When the changes are introduced in April 2027, the clients who will be most impacted will be those who are not leaving benefits to their spouse, are unmarried or without a civil partner, are over 75, and have large funds that they are likely to use during their lifetime, and whose assets are over their Nil Rate Band Allowances.

Plan to reduce your pension scheme values and plan for IHT in the future.

Please remember that past performance is not a guide to future performance. The value of investments and the income from them can go down as well as up and investors may not get back any of the amount originally invested. Exchange rate changes may cause the value of overseas investments to rise or fall.

This is a personal newsletter. Any views or opinions represented in this publication are personal and belong solely to the publication owner and do not represent those of people, institutions or organisations that the owner may or may not be associated with in professional or personal capacity, unless explicitly stated.

All content provided on this publication is for informational purposes only. The owner of this publication makes no representations as to the accuracy or completeness of any information.

The owner will not be liable for any errors or omissions in this information nor for the availability of this information. Nor will the owner be responsible for any actions you carry out as a result of reading the content.

Complaints – If you are dissatisfied, you are entitled to make a complaint. Please be assured we treat complaints seriously. For your further protection, if you cannot settle your complaint with us, you may be entitled to refer it to the Financial Ombudsman Service (FOS). Full details of FOS can be found on their website at www.financial-ombudsman.org.uk

The Premier Partnership Limited is authorised and regulated by The Financial Conduct Authority.
The Premier Partnership Limited is entered on the FCA Register under reference 209446.

5 Pebble Close · Amington · Tamworth · Staffordshire · B77 4RD
T 01283 711222 F 01283 711444 E enquiries@premierpartnership.co.uk W www.premierpartnership.co.uk
Registered Office: 5 Pebble Close · Amington · Tamworth · Staffordshire · B77 4RD