Kingston Smith

Helping clients succeed

Charities Toolkit

A toolkit for managing fraud risks

A toolkit for charities to minimise fraud risk

Benchmarks for an effective fraud risk management framework

1. Understanding what fraud is and how it can arise
2. Adopting an effective Anti-fraud Policy
3. Adopting an effective Fraud Response Plan
4. Implementing robust systems and controls to prevent fraud
5. Adequately recording and reporting fraud

The last report of the National Fraud Authority (NFA), published in 2013, estimated that fraud costs the charity sector over £140m a year. Almost 10% of the charities that responded to the NFA's survey on fraud, 'The Annual Fraud Indicator', had identified fraud in the previous 12 months, with almost half of this relating to payments/banking fraud, followed by accounting fraud and identity fraud.

Charity activities and operations can be prone to fraud for a number of reasons. Many charities rely on a small team of staff, often supported by volunteers, and staff responsible for managing the charity's finances may have little or no supervision. A culture of openness, trust and volunteering has many positive aspects, but may mean controls systems are less stringent than the ideal.

For many charities, the income generated from their activities may be difficult to predict, for example where there are high levels of cash donations from varying events, and income and expenditure streams may not be comparable year on year, making it less easy to identify where results have been skewed by fraudulent transactions. Moreover, with the increase of 'online' activity in the way businesses communicate and transact, this has increasingly opened up new opportunities for fraud to take place.

No charity can assume it is immune to fraud; fraud risk is an important part of any risk management framework. Charity trustees act as the custodian of their charity's funds. They are publically accountable and are bound under charity law (and similarly in company law if the charity is incorporated) to safeguard their charity, its funds and assets. Trustees are ultimately responsible for preventing and detecting fraud within their charity.

This toolkit is aimed at helping trustees and the management team who work with them to understand how charity fraud can arise and looks at ways to mitigate this risk. It also incorporates an action plan to deal with suspected or actual fraud.

1. Understanding what fraud is and how it can arise

In order to be in a position to identify and to predict where fraud is most likely to occur in your organisation, you must first understand what fraud is and what the key motivators are for carrying out fraud.

The Fraud Act 2006 identifies three ways of committing fraud:

- By false representation
- By failing to disclose information
- By abuse of position

And with the intention to act dishonestly in order to:

- Make a gain for the perpetrator, or;
- Cause the loss, or risk of loss to another.

Charities toolkit

What are the key drivers for fraud?

Personal gain: such as where an employee steals money in order to fulfill a financial need. This often starts at a fairly low level and progresses to larger or more frequent instances of similar fraud, so long as the employee's actions continue unnoticed.

Opportunistic fraud: where there is a lack of control, or a culture where low level fraud is ignored, that increases the opportunity for fraud to go undetected and provides the perpetrator with an easy target.

Organised crime: which is more often perpetrated by parties external to the organisation, that have a clear criminal intent and may work through a network to carry out fraud against a number of organisations.

Much fraud is **'insider enabled'**, where the opportunity for fraud arises because someone connected with the charity is given access to the charity's assets and systems, or uses their ability to influence outcomes and decisions for their personal benefit.

'Insiders' will not only be employees and trustees but also include volunteers, who may form a significant workforce for many charities, together with consultants and other contractors.

'Externally enabled' fraud may be harder to detect and is certainly more likely to be perpetrated with little advance warning, so it is important to consider where the potential target areas for your charity are likely to be.

Typically this will include:

- **Banking fraud:** such as cheques being intercepted in the post and diverted to another fraudulent bank account; counterfeit cheques being presented with false signatures; or an external fraudster setting up standing order payments to his/her own bank account
- **Identity theft:** an increasingly common example of this is where a trader improperly uses a charity's name to acquire donated goods through house collections which the trader then sells for personal gain
- **Cyber fraud:** examples include computer viruses and hacking; malware; fake website and email scams; and phishing where the intention is to steal personal or financial data for fraudulent use

Have you considered which of your activities will leave you more vulnerable to fraud?

The opportunities for and risk of fraud will vary from charity to charity but will be affected by its size; the dynamics and competencies of the team that work with and for it; its culture and ethos; the geographical locations of its work; the nature of services provided; how income is generated; and the beneficiaries it supports.

Charities with a small number of staff and a close-knit team may have an increased risk that staff are trusted to 'get on' with their work, without a more formal system of checks and balances that would be in place in a larger organisation.

Charities with a finance officer who has sole charge of financial processing and reporting have an inherently increased risk of financial fraud. All too often when fraud is discovered it is a longstanding and highly regarded member of the team that has taken an opportunity to divert charity funds or to abuse access to say a company credit card.

External fraud is most likely to arise where there is inadequate control over purchasing and supplier accounts, and over data security. Cyber crime is an aspect that is increasingly affecting charities that commonly retain significant personal information about their beneficiaries and donors.

Take a good look at your operations to identify those that may leave your operations more vulnerable to fraud. The following are typically operations that tend to increase fraud risk:

- Working internationally in areas where there are likely to be less stringent control systems in place or an attitude that is more open to bribery and corruption
- Having a high volume of cash income streams, or reliance on third parties to generate income on your behalf
- Using a large number of volunteers to undertake work for the charity
- Undertaking trading activity through charity shops, and holding stocks of goods for sale
- Utilising a branch network, particularly where branch activity is volunteer led
- Having a small finance team and/or staff who operate unsupervised, particularly over banking and payment functions
- High activity on company credit cards or throughput of petty cash transactions
- Holding beneficiary and donor data on an internal database or relying on a third party to manage this for you
- Transacting with individuals or companies that are connected to staff or trustees of the charity

Do you actively look out for signs of fraud and appraise the risks?
Fraudsters are inventive, so it pays to actively watch out for potential new fraud risks and to consider regularly the impact of changing operations and circumstances on internal control systems. Don't underestimate the potential impact of cyber crime where the penalties for inadequately protecting data can be significant.

Take steps to ensure that Trustees and staff alike are aware of and can spot warning signs that might indicate that a fraud has taken place.

Remember though to consider these within the context of other operational circumstances that might ultimately confirm there is another rational explanation that excludes fraud. Don't jump in with accusations before you have evidence to support initial indications of fraud.

Outlined in Appendix A are some common potential indicators of fraud. Use these to measure your own charity.

2. Adopting an effective Anti-fraud Policy

Does your charity have an appropriate anti-fraud policy?
A robust anti-fraud policy will particularly help your charity to prevent 'insider enabled' fraud by providing a clear indication to staff and those that work with them that fraud is taken seriously. It should provide a message that fraud is not acceptable and that all possible steps are being taken to eradicate the chance of fraud occurring in the charity, which in itself should act as a deterrent to fraud.

As a minimum, an anti-fraud policy document should include:

- A commitment to prevent, detect, investigate and report fraud
- An explanation of the role of the trustees, management and employees in preventing and reporting fraud or suspected fraud
- An explanation of how the charity assesses its exposure to and management of fraud risk
- Reference to the interaction with any internal audit function in place
- A response plan that indicates the steps to be followed in the event of fraud being suspected or detected.

An example of an anti-fraud policy document is found in Appendix B.

Do your staff and trustees understand and adhere to the policy?
There is no point in having an anti-fraud policy if it's not communicated to those who work for the charity, or understood by all that fraud cannot be tolerated.

Employees should be in no doubt of the sanctions that will be applied if they commit fraud.

Vetting checks need to be robust. In particular consider the use of credit checks and screening for staff involved in finance roles or who make financial decisions on behalf of the charity.

The Bribery Act 2010 reinforced the position in law that the giving or receiving of bribes is a criminal offence and is considered a form of fraud. Charities need to be on guard against staff or trustees who are influenced in a manner that affects their ability to put the needs of the charity first. Formulation of an anti-bribery policy goes hand in hand with your anti-fraud policy.

The charity's whistleblowing policy needs to incorporate a clear process for reporting concerns about fraud and other criminal acts that encourages communication whilst maintaining confidentiality and provides a support mechanism for the whistleblower.

3. Adopting an effective Fraud Response Plan

Do you have a clear plan to manage suspected or actual fraud?
The more quickly and decisively you can respond to an instance of suspected fraud, the more likely you are to be able to prevent further loss and to mitigate the reputational impact for the charity.

Any Fraud Response Plan needs to identify clearly the timescale for action. Some actions such as the decision to report the fraud to Action Fraud, The Police and the Charity Commission, must be taken immediately, as will the need to review security systems to prevent further loss.

The strategy for communication is particularly important as this must take account of legal requirements, for example to preserve data security, but it is also vital that employees and staff are aware of the need to stick to an agreed reporting brief and to channel external communication through an appropriate individual such as the Chair of Trustees.

Develop a Fraud Response Plan that identifies the following:

- Responsibilities for following up and investigating a suspected fraud
- Who needs to be contacted internally and externally in the event of fraud and in what circumstances
- Procedures to be undertaken to review and lock down systems to prevent further fraud
- The framework for any internal investigation into fraud
- The process for assessing the impact of the fraud and acting on lessons learned
- Record keeping requirements in relation to fraud

An example of a Fraud Response Plan is found in Appendix C.

How will you address the impact of any fraud loss?
When a fraud is discovered, the trustee board's priority should be to establish the facts that will form the basis of reporting to relevant authorities and to assess the impact of the loss to the charity. The board is not responsible for determining whether a criminal offence has been committed.

It is vital to consider the impact of the loss from a financial and non-financial perspective:

- Make sure you have thought about who will be responsible for quantifying the loss (which may need the help of external consultants, your auditors or forensic accountants)
- Consider how the loss will be reflected in your financial statements and whether there is a significant effect on the charity's funds and its future financial viability – this will in turn have an impact on how comfortable funders and partners are in continuing to work with the charity in the future.
- Consider any potential route to recovery and the likely costs associated with this
- Identify lessons to be learned from the way the fraud was perpetrated that pinpoint weaknesses in systems and controls and ensure these are tightened and improved
- HR processes will need to be carefully followed to ensure any disciplinary action taken meets the required legal framework.

4. Implementing robust systems and controls to prevent fraud

Charities are in a unique position in that they have a trustee board who oversee the strategy and financial well-being of the organisation whilst leaving day to day operations to a management team.

Charities trust their team to work in the best interests of the charity and the public entrust the charity with using their money to undertake charitable work.

Trustees and staff must take their responsibility to prevent fraud extremely seriously and in doing so, the trustees have ultimate responsibility for establishing proper and robust internal controls and operating systems.

Have you evaluated the adequacy of your systems of internal control?
Internal control systems need to be appropriate for the size and complexity of the charity, the risks it is exposed to and the nature of its operations. Consider whether your charity has appropriate levels of control that are clearly set out in an internal controls and procedures document or manual.

Staff should be fully aware of the controls and processes relevant to their department or team and have access to the control procedures manual for reference.

Appendix D provides a checklist covering key aspects of internal control that charities should consider when assessing strengths and weaknesses in their internal control systems.

Conclusion

A robust approach to considering and managing fraud will contribute significantly to the sound governance of any charity and plays an important part in effective risk management.

The trustee can take comfort that they are properly fulfilling their duties to safeguard the charity's assets and funds and to prevent and detect fraud.

Staff will understand the need to maintain the highest standards of integrity and honesty in their work and actions.

Taking robust action on fraud will help to limit the reputational damage that might otherwise ensue.

5. Adequately recording and reporting fraud

Do you keep a log of all incidents of fraud?
In fulfilling their duty to safeguard the charity's assets, trustees must not underestimate the importance of adequately documenting instances of fraud.

In assessing the seriousness of incidents, it is easy to overlook the fact that low level fraud can build into a more significant issue if perpetrated regularly without detection. By keeping a full record of suspected or actual fraud, this enables the trustees and staff to track and identify repeat instances. It also ensures that there is an adequate audit trail of incidents and actions to support any reporting requirements and provides evidence that the board has responded in an appropriate manner to identified incidents.

Do you know who to report fraud to?

- **Action Fraud** – www.actionfraud.police.uk
  Fraud should always be reported to Action Fraud and each reported fraud is given a police crime reference number.
- **Local Police** – www.police.uk
- **Charity Commission** – www.charitycommission.gov.uk/running-a-charity/your-charitys-work/protecting-your-charity/reporting-serious-incidents

The Charity Commission provides detailed guidance on reporting fraud in its publication '*The Reporting of Serious Incidents – Guidance for Trustees*' and requires that serious incidents are reported as soon as they are suspected.

Remember that where a charity has annual income exceeding £25,000, the trustees have a statutory requirement to provide a declaration when submitting the charity's Annual Return, that all serious incidents in the previous financial year have already been reported to the Charity Commission.

Other bodies you will need to consider notifying will depend on the particular circumstances surrounding the fraud. For example you will need to contact the charity's bank if there is an issue involving fraudulent access to your bank account, or HMRC if the fraud is linked for example to gift aid or VAT.

Practical guides & templates

To accompany this toolkit we have provided a series of guides and templates to support you to develop a robust framework for fraud risk management:

A – Potential Indicators of Fraud
B – Example Anti-fraud Policy
C – Example Fraud Response Plan
D – Internal Control Assessment Checklist

These do need to be adapted to fit the size and structure of each entity but the following should be used a general guide for further consideration.

Appendix A
Potential Indicators of Fraud

Ensure staff and trustees have an understanding of what to look out for and are aware of early warning signs such as these listed below:

Employment related indicators:

- Certain employees regularly working longer hours than others, or not taking their given quota of annual leave
- Employees with a sudden and unexpected improvement in lifestyle or personal spending habits
- Employees who appear constantly stressed or who become aggressive or defensive when questioned about their work
- Employees who are unable to provide information or answers requested, including failing to support expense claims with valid vouchers
- Employees who look to delay internal audit or other similar inspections
- Rapid staff turnover for no apparent reason
- Employees or trustees who have failed to declare connected business interests
- Employees or trustees who have provided inaccurate information on their CVs

Financial and operational indicators:

- Un-reconciled account balances (such as bank, supplier and customer control account reconciliations) or unexplained differences linked to cash activity
- Changes in costs or revenues that are out of line with budgets and expected margins
- Unusual or unexplained transactions linked to journal entry postings or inter-company account transfers
- Higher than expected refunds or credits against customer accounts
- Higher than expected losses on cash/till takings or on inventories
- Financial records that contain many copies rather than original documents or where documents appear to have been altered
- Payee names appearing regularly that are not known suppliers
- Missing financial records, cheque books/ cheques or pre-signed cheques
- Use of persons/companies connected to staff or trustees to deliver services or receiving regular payment
- Asset register that doesn't match to physical assets held
- Over reliance on one individual to manage financial transactions (i.e. lack of adequate segregation of duties over receipt and banking of funds/authorisation of and payment for purchases)
- Excessive customer complaints
- Lack of control over delegated procedures and reporting mechanisms for review of work done, or controls not operating as expected
- Lack of adequate internal control checks commensurate with the size and complexity of the organisation

Appendix B
Example Anti-fraud Policy

As with all risk management processes your anti-fraud policy needs to be reviewed regularly to take account of changing circumstances and activities, together with any external factors that might affect the incidence or risk of particular fraud to your charity.

Anti-fraud policy for Charity XXX

1. As a UK registered charity we undertake to comply with UK law relevant to countering fraud including Company Law (*if incorporated*), Charity Law, the Fraud Act 2006 and the Bribery Act 2010.
2. The purpose of this statement is to give charity XXX's policy on fraud and set out our responsibilities for its prevention.

What is fraud?

3. Fraud covers a range of activities including deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, false accounting, concealment of material facts and collusion. It includes the use of information technology equipment to manipulate programs or data dishonestly, the theft of IT equipment and software, and the intentional misuse of computer time and resources.
4. In essence fraud involves the intention to act dishonestly in order to:
   - Gain a personal advantage, financial or otherwise, for the perpetrator and/or those connected to him/her, or
   - Cause the loss, or risk of loss to charity XXX
5. Fraud can be perpetrated by employees, officers, trustees, directors, volunteers and any others acting on behalf of the charity including agents and contractors.

Who is covered by this policy?

6. This policy applies to the trustees, employees, volunteers and all other individuals working within or on behalf of charity XXX. Charity XXX is also required to take appropriate steps to establish that the Partners and Associates with whom charity XXX works comply with anti-fraud regulations in line with the terms of this stated policy.
7. In compliance with this policy charity XXX requires all connected individuals (as listed above) at all times to act honestly and with integrity and to safeguard the resources for which they are responsible. The threat of fraud must be a concern to all members of staff as well as the board of trustees.

Who is responsible for this policy?

8. The Board of Trustees has responsibility for ensuring that this anti-fraud policy is appropriate and adequate in minimising the risk of fraud and that they lead by example in establishing a culture of abhorrence of fraud in any form throughout the organisation.
9. XXX (*e.g. Head of governance or other designated person*) has day-to-day responsibility for implementing this policy and monitoring its effectiveness.
10. Employees are responsible for adhering to the terms of this policy and for reporting suspected instances of non-compliance with it.

Prevention of fraud

11. We undertake to establish procedures that deny the opportunity for fraud to take place. These will include: proper leadership; robust internal financial and operating control systems; sound internal and external audit reviews; appropriate trustee/employee/volunteer and contractor screening and vetting procedures.
12. Charity XXX will undertake to carry out thorough and prompt investigation of suspected fraud and to take appropriate disciplinary or other appropriate action against the perpetrators of fraud or attempted fraud.
13. Individuals working within charity XXX are required to:
    - Identify and assess the risks of fraud involved in the operations for which they are responsible;
    - Alert their line manager where they believe that the anti-fraud policy is at risk whether through poor procedures or lack of adherence to the principles of this policy;
    - Report details of any suspected or actual fraud to their line manager in the first instance. Consideration of when it may be appropriate to report under charity XXX's whistleblowing procedures and to whom it is reported is outlined at XXX. (*refer to policy documentation on whistleblowing here*)
14. Employees who breach this anti-fraud policy will be subject to disciplinary action, which may result in dismissal. We reserve the right to terminate contractual relationships with Partners and Associates who breach this policy.
15. All employees will receive induction and regular further training on how to implement and adhere to this anti-fraud policy.

Monitoring and review

16. The Board of Trustees will monitor the effectiveness of the policy, its suitability and proper implementation at least annually. XXX (*The Head of Governance or other designated person*) will undertake regular checks of control systems and procedures undertaken, utilising internal audit as appropriate, to obtain assurance that they are appropriate and adequate in minimising the risk of fraud.

Appendix C
Example Fraud Response Plan

This template will need to be tailored to fit the size and operational structure of your charity. Smaller charities may have much simpler lines of reporting and communication than outlined below.

Fraud Response Plan for Charity XXX

The purpose of the Fraud Response Plan is to outline the procedures to be undertaken in the event of a suspected or actual fraud taking place.

It defines the roles of those involved and confirms the lines of communication and reporting of fraud and will help to ensure that the charity XXX is well prepared to deal with fraud in an effective and efficient manner.

Immediate action to be taken

1. In the event of a suspected or actual incidence of fraud the person who has identified this should report this to their immediate line manager.
2. The line manager will report in turn to their direct line of reporting within the Senior Management Team who will in turn inform the CEO.
3. The CEO will notify the Chair of the Board of Trustees and the Chair of the Audit and Governance Committee.
4. The nominated sub group responsible for dealing with fraud will convene, if necessary by teleconference or other similar means, in order to determine:
   - The action to be taken to minimise any immediate or further loss to the charity, who will implement these and by when.
   - The Agencies that must be communicated with first, including Action Fraud and The Police.
   - The steps to be taken to investigate the fraud, including the need to call external expertise such as from forensic accountants, internal auditors, HR support and legal advice.
   - Whether the charity's own investigations must await the outcome of any police investigation.
5. Where a member of the nominated sub group is themselves implicated in the fraud, care must be taken to ensure they are excluded from these discussions and that another persons is appointed in their place on the nominated sub group.
6. Ensure all relevant security passes, keys and charity assets such as laptops and company phones are returned and ensure access to systems is withdrawn for the individual(s) concerned.

Secondary action within the next 48 hours

7. Determine the communication strategy for internal and external communication; the key person who will make such announcements as are deemed necessary and appropriate; and the timing of these.
8. Follow through on initial findings to determine whether there are likely to be further losses and agree a process/ investigation framework to establish the scale of the losses and the financial impact.
9. Determine whether advice needs to be taken on legal matters related to employment law and/or data protection.
10. Establish whether any staff member(s) should be suspended and take necessary action.
11. Determine the extent to which other parties such as the Charity Commission and HMRC will need to be informed of the fraud.
12. Ensure the mechanism for recording the fraud and actions taken to respond to it is initiated.
13. Draw up a communication plan for external stakeholders.

Follow up action

14. Obtain advice as necessary on the actions to be taken to recover losses and pursue these with the charity's insurers and/or with legal support if necessary.
15. Determine the extent to which other costs connected to the loss may be recovered.
16. Continue to communicate regularly with the full Board of Trustees and Senior Management Team as to the outcome of investigative work.
17. Undertake appropriate disciplinary action/follow up on any staff dismissals.
18. Assess the impact of the loss both financially and for the charity's reputation.
19. Evaluate and act on lessons learned to tighten systems and to establish new processes to improve risk management of fraud. This needs to encompass consideration of financial, IT and operational controls and the role of internal and external audit in supporting this.
20. Follow up to ensure actions for change are implemented within the desired timescale.

Appendix D
Internal Control Assessment Checklist

Charities should regularly undertake and reassess the key fraud risks that are relevant to their activity and assess whether their internal control systems still adequately meet their needs. Use the checklist of questions below to assess the strengths and weaknesses in your internal control systems.

Charity XXX internal control assessment	Yes/No
1. Financial records should be robust enough to ensure that they capture all financial data and that they identify separately restricted and unrestricted income and expenditure	
2. There should be adequate underlying records including invoices, receipts and expense vouchers to support all income and expenditure	
3. Income and expenditure should be used to further the aims of the charity and for no other purpose	
4. There should be adequate segregation of duties particularly between receiving, banking and recording income and between raising of expense orders, approval and payment	
5. There should be expenditure approval value limits and multiple signatories over bank payments whether by cheque or online	
6. Accounting records should be kept up to date and control accounts regularly reconciled over bank balances, debtors and creditors ledgers, payroll related costs, and PAYE and VAT liabilities	
7. Access to financial and other information should be password protected and limited according to the responsibilities and seniority of individuals accessing it	
8. There should be spot checks on records and systems and a review of 'exception' reports (for example of changes to payroll details or new suppliers). In particular the aim here should be to identify financial controls that have been ignored or bypassed	
9. Opening and closing bank accounts and changes to bank mandates should only be approved and initiated at trustee level	
10. Fixed asset registers should reconcile to accounting records and to physical assets	

Appendix D
Internal Control Assessment Checklist

Charity XXX internal control assessment (continued)	Yes/No
11. Valuable assets should be securely held in a safe or in a locked or alarmed location with restricted access requirements, including log-ins and passwords clearly understood and followed	
12. Trustees, employees, volunteers and contractors should be properly vetted and their skills and capabilities assessed	
13. All individuals who work for and with the charity, including volunteers, should understand their role, have adequate training to carry this out effectively and have proper channels for reporting and review of work undertaken	
14. Financial management reporting should be regular, timely and tailored to the needs of the user, with detailed information for budget holders and Senior Management Team and higher-level summaries for the board. This should include comparison of income and expenditure with budgets, balance sheet analysis including restricted and unrestricted funds, cash flow projections and reforecast results to the anticipated period end	
15. Protection and security of database information, website portals and system networking must comply with legislative requirements and be sufficiently robust to prevent data loss or leakage. The security needs to be monitored and tested regularly, which will often require specialist IT support	
16. There must be proper control of outsourced functions (for example a membership fulfillment system) where a third party manages invoicing and renewals on a day-to-day basis. There is an important difference between a 'data controller' who is responsible for personal data that it holds and a 'data processor' who holds personal data, but processes it under the instructions of the data controller and where this data remains the responsibility of the data controller	
17. There must be proper protection of personal data flowing between group companies (such as sharing of data base contact information). Each group company will still have its own legal data protection responsibilities and it is important to understand when and how personal data may be shared between group companies	
18. There should be effective output from internal and external audit functions which is followed through appropriately	

Contact us

More information about Kingston Smith services to the charities sector can be found at www.kingstonsmith.co.uk/charities

City
Devonshire House
60 Goswell Road
London
EC1M 7AD
T 020 7566 4000

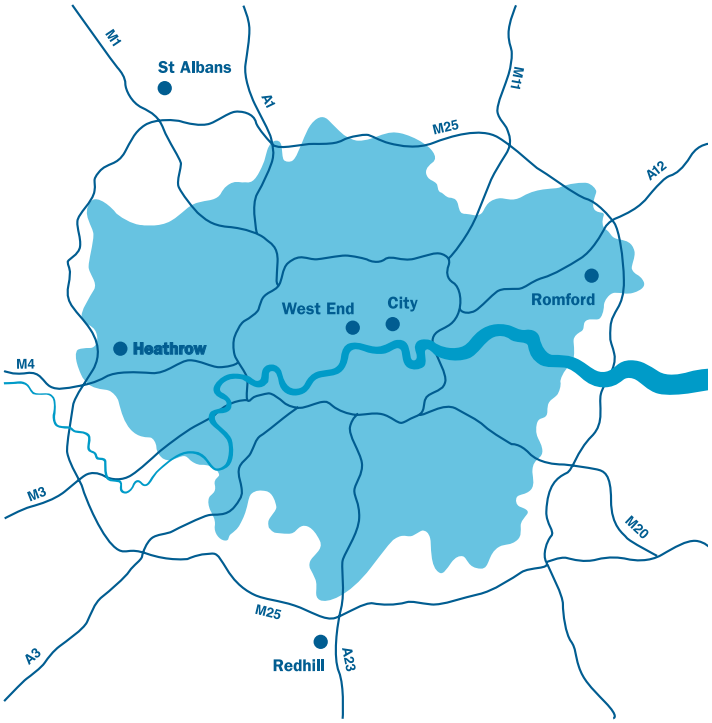
Heathrow
Middlesex House
800 Uxbridge Road
Hayes, Middlesex
UB4 0RS
T 020 8848 5500

Redhill
Surrey House
36-44 High Street
Redhill, Surrey
RH1 1RH
T 01737 779000

Romford
Orbital House
20 Eastern Road
Romford, Essex
RM1 3PJ
T 01708 759759

St Albans
105 St Peter's Street
St Albans, Hertfordshire
AL1 3EJ
T 01727 896000

West End
141 Wardour Street
London
W1F 0UT
T 020 7304 4646



For further information on Kingston Smith and our services please visit our website: www.kingstonsmith.co.uk

Kingston Smith
Helping clients succeed