Information Brief

Winter 2011

In this issue

Welcome

Welcome to the first edition of the Devonshires I-Brief.

We have been advising our clients on data protection and freedom of information issues for many years now, but with the growth of the internet, Twitter and other social networking sites as well as advances in information storage and retrieval, we have seen a significant increase in the number of clients seeking advice on information law issues.

From inadvertent breaches of data protection to vexatious requests under the Freedom of Information Act, information law represents a challenge to all our clients. And if the Government's proposal to include private registered providers in FOIA goes ahead next year, our clients are going to have to grow their knowledge and skills in this area – and quick!

The members of the Devonshires' Information Team are all experienced in advising on information law issues. Profiles of the team members appear at the back of this issue. We are also excited to launch our new freephone Information Helpline which gives clients access to speedy, solution-driven advice on information law issues.

In this first edition of I-Brief, we bring together a number of relevant articles on matters of the moment which we hope you will find informative, if not entertaining.

Happy reading!

Nick Billingham, Partner

20 things you need to know about the Freedom of Information Act

If, following the Ministry of Justice consultation, private registered providers are brought within the scope of the Freedom of Information Act, you will need to be fully prepared to respond to the challenges that this will pose and ensure that you can comply with its obligations.

Below we set out 20 things you will need to know about the Act:

1. If the Act is extended to Registered Providers it will be by an order of the Secretary of State which will specify the functions which are to be included in the scope of the Act. The Act will not apply to information relating to any functions which are not specified in the order.
2. The Act is fully retrospective and will therefore apply to information whenever it was created and not just information created after the Act came into force.
3. Requests for information made under the Act normally have to be complied with within 20 working days of receipt.
4. If information requested under the Act falls within an exemption then a public authority may not need to release that information. There are two types of exemption – absolute and qualified.
5. If an absolute exemption may apply the only question is whether or not the exemption does apply and if it does then the information in question does not need to be disclosed.
6. Qualified exemptions on the other hand are subject to a public interest test which means that a public authority has to consider whether the public interest in not disclosing the information outweighs the public interest in disclosing the information - if it does then the exemption will apply. There is though a presumption in favour of disclosure.
7. If a qualified exemption may apply and the authority is considering the public interest

test then the 20 working day time limit is relaxed and requests should be complied with within 'such time as is reasonable in all the circumstances'. The Information Commissioner has stated that 40 days should be the maximum length of time needed in these circumstances.

8. The Information Commissioner advises that when applying the public interest test only those considerations relevant to the exemption being claimed should be considered (and not general public interest considerations) and the test needs to be considered separately for each exemption which is being claimed.

9. If exemptions are to be relied on they must be cited for each piece of information which is being withheld – if an exemption only applies to part of the requested information then the exempt information should be redacted. When redacting information a public authority must justify each individual redaction by reference to an exemption and explain why it applies.

"Public authorities have a duty to provide advice and assistance to those who have made or propose to make a request for information"

10. If information is to be withheld the applicant must be given a refusal notice.

11. If someone wants to see their own personal information, the existing rights under the Data Protection Act still apply.

12. A public authority does not have to comply with a request if the cost of doing so would exceed the 'appropriate limit' which is currently £600 for central government bodies and £450 for other public authorities. Time can be charged at £25 per hour but only limited activities can be taken into account – for example time spent considering exemptions that may apply and in redacting exempt material cannot be included.

13. Public authorities may refuse requests that are vexatious. The Information Commissioner advises that this must be considered by reference to the request itself and not the requester.

14. Public authorities do not have to respond repeatedly to the same or similar requests from an applicant.

15. Public authorities have a duty to provide advice and assistance to those who have made or propose to make a request for information.

16. Public authorities must adopt publication schemes and publish information in accordance with their scheme.

17. The right of access only relates to information which is 'recorded in any form' so will not extend to unrecorded information.

18. The right applies to information which is held by a public authority and this includes information held by another person on behalf of the authority. Information which an authority holds on behalf of another person is though expressly excluded.

19. If a public authority refuses to disclose information and the applicant has exhausted any complaints procedure provided by the public authority then the applicant can appeal to the Information Commissioner - appeals from the Information Commissioner are heard by the First Tier Tribunal and appeals from this tribunal are heard in the Upper Tribunal and then the Court of Appeal.

20. Where public authorities repeatedly or seriously fail to meet the requirements of the Act, or conform to the associated codes of practice, the Information Commissioner has the power to take a range of action including:

    a. Conduct assessments to check an organisations compliance;

    b. Issue undertakings committing an authority to a particular course of action to improve its compliance;

    c. Serve enforcement notices where there has been a breach of the Act, requiring organisations to take specified steps;

d. Issue decision notices detailing the outcome of the Information Commissioner's investigation to publically highlight particular issues; and

e. Prosecute those who commit criminal offences under the Act – in particular where a request for information has been received it is an offence to alter, deface, block, erase, destroy or conceal any records held by a public authority with the intention of preventing disclosure of that information under the Act.

Elen Storey is a solicitor in Devonshires' Projects Group. She specialises in Freedom of Information issues particularly in the context of public/private partnerships. Elen can be contacted on elen.storey@devonshires.co.uk or 020 7880 4389.

Under scrutiny: Planning decisions for historic buildings

Devonshires works closely with specialist Information Law barristers. From time to time challenges under the Data Protection Act and FOIA reach the Information Tribunal when the advocacy skills of such barristers are needed. Robin Hopkins of 11 KBW is one of the barristers we work with. Robin writes here about a recent Information Tribunal on a planning decision.

A recent Information Tribunal ruling suggests that when it comes to planning decisions relating to historic buildings, public scrutiny trumps commercial confidentiality. However, the judgement has left a number of unanswered questions.

To local authority lawyers involved in planning or information law, the pattern will be all too familiar. A developer applies for planning permission to demolish or convert a historic building. In accordance with statutory guidance, the application is accompanied by a report purporting to show alternative use of the current building to be unviable.

Objectors understandably wish to interrogate this 'viability report', and they request a copy under the Environmental Regulations 2004, the younger sibling of the Freedom of Information Act 2000. The developer wishes to keep any sensitive commercial data contained in the viability report confidential. The sympathetic local authority therefore refuses to disclose the report, relying on the relevant exemption (regulation 12(5)(e)) under the EIR. In such circumstances, which takes precedence: commercial confidentiality or public scrutiny? Following the Information Tribunal's recent decision in Bristol City Council v IC and Portland and Brunswick Squares Association (EA/2010/0012), the answer would appear to be the latter.

The Tribunal was – as Tribunals tend to be – at pains to deny that it was setting a broad precedent for full transparency in planning applications. Nevertheless, the upshot, in my view, is that it will now be very difficult to withhold viability reports or any other information which will be decisive in a planning decision about a historic building. This is arguably the most significant development in the intersection of planning and information law since the 'Vauxhall Tower' decision of 2007 (*Baker v IC and Dept for Communities and Local Govt (EA/2006/0043)*).

In order to digest and apply this case in practice, close attention to the underlying facts is required. First, the buildings: a Coroner's Court (Victorian; grade II listed; refurbishment and conversion proposed; in council ownership but with a conditional contract for sale to the developer) and an adjacent site (also Victorian; not listed, but in a conservation area; demolition proposed; already owned by the developer).

Next, the documents at issue: one was the developer's viability report, the conclusion of which had been officially pronounced "not unreasonable" by an independent quantity surveyor. The second was a 'feasibility costs report' submitted by the developer. In short, the disputed information included the developer's estimates as to both the costs of and the returns on alternative schemes for the site.

The chronology should also be noted: the Residents' Association's request for information was finally refused in April 2008. That was therefore the relevant date from an EIR perspective. Planning permission was granted in June 2008, but was swiftly subject to a judicial review challenge. The JR proceedings in turn were stayed pending the Information Tribunal's decision.

Finally, the applicable planning guidance was PPG15, which provided that a listed building could only be demolished where there was "clear and convincing evidence that all reasonable efforts have been made to sustain existing uses or find viable new uses and these efforts have failed… or that redevelopment would produce substantial benefits for the community which would decisively outweigh the loss resulting from demolition" (paragraph 3.17).

As we shall see, the stringency of this test was fundamental to the Tribunal's finding in this case. PPG15 further provided that proposals to demolish unlisted buildings which make a positive contribution to the character or appearance of a conservation area (as was agreed to be the case here) should be assessed against the same broad criteria as listed buildings (paragraph 4.27).

PPG15 has of course since been supplanted by PPS5, which retains a reconfigured version of the aforementioned principles, albeit with a hint of uncertainty about unlisted buildings in conservation areas (of which more anon). With the foregoing facts in mind, we can examine the Tribunal's reasoning on the engagement of the exemption and the public interest balance.

"The explicit and information-specific (rather than blanket) signposting of an expectation of confidentiality will, however, help to make the engagement of regulation 12(5)(e) less contentious"

Contrary to the Information Commissioner's decision, the Tribunal found that the exemption under regulation 12(5)(e) was engaged, notwithstanding the absence of any express reference to confidentiality in the correspondence or documents themselves, because the desire to cloak an economic interest in confidentiality was implicit in the context. The explicit and information-specific (rather than blanket) signposting of an expectation of confidentiality will, however, help to make the engagement of regulation 12(5)(e) less contentious.

The public interest factors favouring disclosure were listed as: (i) the viability report being a "major factor" in (ii) a controversial decision; (iii) the requirements of PPG15; (iv) the planning regime's emphasis on the engagement of local residents, amenities societies and other interested parties; (v) the "particular scrupulousness" demanded of a Council when dealing with one of its own sites, and (vi) the mismatch in resources between the Council/developer on the one hand and the Residents' Association on the other (the latter could not afford to commission a separate viability report of their own).

The public interest in maintaining commercial confidentiality was noted, but downgraded in this case due to a number of factors. Some were fact-specific but common enough: the absence of any express insistence on confidentiality by the developer, and the viability report's use of general pricing levels in the construction industry and "hypothetical" (as opposed to actual) forecasts. The latter is a little mystifying, given that forecasting is an intrinsically hypothetical activity. In any event, "the most telling factor" against disclosure – namely that developers might refuse to supply viability reports if publicity is envisaged – was discounted because, where PPG15 applies, there simply cannot be a reasonable expectation of confidentiality.

In the end, it was not a close-run affair: the Tribunal found that the public interest in disclosure "substantially outweighed" that in maintaining the exemption. In the circumstances of this case, that decision must be right.

We can go further: a quick glance through the factors listed above reveals that the majority will apply to any planning decision about a historic building – hence the prescriptive force of this decision. Note this conclusion from the Tribunal: "so far as PPG15 viability reports are concerned, it seems to us that developers will not be able to refuse to supply them if they want to obtain the relevant consent but that, given their hypothetical nature, it may be possible for them to construct such reports in a way that does not reveal sensitive commercial information specific to themselves". It is not entirely clear how this suggestion is to be implemented.

Further uncertainty comes from the Tribunal's observation that "the result may have been different, for example, if the information had not been provided to satisfy the PPG 15 criteria or if the Council had not owned the Coroner's Court building".

This has two odd implications. One is that for historic buildings in *private* ownership, commercial confidentiality could prevail over the public interest in disclosure. The other is that if the building in question had been publicly owned but non-historic, the Tribunal may still have reached the same conclusion. Given how large PPG15 loomed in this decision – compared with the question of public versus private ownership – both of these implications should be approached with caution.

"If a building is publicly-owned but not historic, disclosure may be required; if it is historic but privately-owned, disclosure is very likely to be required, and if it is both historic and publicly-owned, disclosure is...virtually unavoidable."

A safer approach might be something like this: if a building is publicly-owned but not historic, disclosure may be required; if it is historic but privately-owned, disclosure is very likely to be required, and if it is both historic and publicly-owned, disclosure is (barring exceptional circumstances) virtually unavoidable. In all cases, the more controversial the planning application, the greater the public interest in transparency.

This unearths another question. PPS5 is expressed in terms of "heritage assets" rather than "buildings". It is as yet unclear whether, in the case of a conservation area, the relevant heritage asset is the area as a whole (in which case the stringent test for demolition need not necessarily apply on a building-by-building basis), or whether each constituent building is itself a heritage asset (in which case the stringent test applies each time, and disclosure is likely to be required).

The first planning inquiry decision to straddle the PPG15 and PPS5 worlds (The Turnmill, 63 Clerkenwell Road, London (APP/V5570/E/09/2118167 and APP/V5570/A/09/2118166)) was not required to resolve this point. My prediction is that the Information Commissioner and Tribunal will presume the stringent test to apply until planning law says otherwise, or unless they are persuaded that the particular building in question is of insufficient merit to justify the level of public interest implicit in PPS5.

For those troubled by the unresolved questions from this crucial decision, I have tried to set out some rules of thumb in this article. In any event, it is safe to say that the Information Commissioner or Tribunal will be asked to wade into another controversial planning decision before too long.

Robin Hopkins is a barrister at 11KBW Chambers www.11kbw.com). He specialises in information, public and employment law.

Is Big Brother watching you?

There are many reasons why employers wish to monitor their employees at work including monitoring performance, preventing theft, and preventing misconduct. However, employers risk breaching employees' trust and privacy if key steps aren't followed.

Part III of the Information Commissioner's Data Protection Code (Code of Practice) focuses on monitoring in the workplace. The Code of Practice is not legally binding and failure to comply with the Code does not automatically mean that an employer has breached the Data Protection Act 1998 (the Act). However, if a complaint has been made to the Information Commissioner it will use the Code of Practice as a standard which the employers practices will be judged by.

Monitoring in the workplace

Monitoring in the workplace can take various forms such as the monitoring of internet usage, websites visited, telephone calls, and vehicle tracker devices. The general starting point is that it would be intrusive to monitor employees at work as they have an expectation to a private life and are entitled to a degree of privacy at work. Furthermore, in every employment relationship there is the implied term of trust and confidence which provides that neither party will undermine the trust and confidence of the other. In the most extreme situations, unjustified monitoring by the employer could lead to a breach of the implied term of trust and confidence and entitle an employee to resign and claim constructive dismissal.

Employers must therefore find a balance between employees' expectation of privacy and what the monitoring will seek to achieve. One way for employers to demonstrate that they have carried out this exercise is for an impact assessment to be carried out prior to the implementation of any monitoring.

Impact assessments

An impact assessment should consist of the following:

- Clearly identifying the purpose behind the monitoring and the benefits which it is likely to deliver.
- Identifying the likely adverse effect on others.
- Considering the alternatives to monitoring (is there a less intrusive way of carrying out the monitoring?).
- Taking into account the obligations that arise from monitoring.
- Assessing whether the monitoring is justified.

Once an employer has carried out the above assessment it will be able to take a view on whether the monitoring is justified. If the employer believes that the monitoring is justified the next step is for the employer to notify the employees how and why they will be monitored. If monitoring is used to enforce an organisation's standards and rules, this must be clearly set out in a policy which should be brought to the workers' attention and which refers to the nature and extent of any monitoring.

"If the employer believes that the monitoring is justified the next step is for the employer to notify the employees how and why they will be monitored"

Covert monitoring

In certain situations employers may wish to adopt covert monitoring in the workplace. The Code of Practice provides that covert monitoring should not normally be considered by an employer as it will be rare for an employer to be able to justify its use. Employers may only consider covert monitoring if there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals of the monitoring would prejudice its prevention or detection.

Rather unhelpfully there is no definition of 'equivalent malpractice' in the Code of Practice. However, it has been suggested that if the employer suspected malpractice of such seriousness that it would entitle an employer to notify the police (even though they do not actually do so) this would be sufficient to justify covert monitoring.

When considering whether to implement covert monitoring an employer must ensure that the decision is taken by a senior level of management and an impact assessment must also be carried out. The key issue, especially with covert monitoring, is that the monitoring must be proportionate. If an employer suspected an employee of stealing stock from a warehouse and it wished to use covert CCTV to monitor the stock room it would not be appropriate for the employer to secretly film the warehouse continuously. In this situation the employer should only film the warehouse on the days or times the relevant employee is working there. This will limit the potential adverse effect on other employees not suspected of theft.

There are essentially two key steps to follow when undertaking any type of monitoring in the workplace. The first is to carry out an impact assessment to establish whether it is justified. The second is to ensure that employees are made aware of how and why they will be monitored in the workplace. It is now more important than ever for employers to ensure compliance with the Act as the Information Commissioner now has the power to fine data controllers up to £500,000 for the most serious breaches.

Ronnie Tong is a solicitor in Devonshires' Employment Team. He specialises in contentious employment issues including data protection breaches and data protection challenges by employees. Ronnie can be contacted on ronnie.tong@devonshires.co.uk or 020 7880 4335.

Naming and shaming: publishing details of tenants subject to court judgements

Many social landlords publish summaries of judgements in their favour to demonstrate that problems are being addressed and to deter their recurrence. Sometimes, publishing the identity of the tenants involved will make this more effective. We have recently been asked to advise on whether landlords can do this.

Whilst judgements given in open court may be considered public, publication will be from the landlord's subsequent records. Landlords are data controllers for the purposes of of the Data Protection Act and any personal data held in their records will be covered by it. Many landlords therefore err on the side of caution and only publish anonymised details.

However, in *R (on the application of Stanley) v Metropolitan Police Commissioner, Brent LBC, Secretary of State for the Home Department* (Stanley v Brent), it was found that a local council could publish photos and other details of those issued with ASBOs on the grounds that this would assist in informing and reassuring neighbours, in enforcing the orders, and in deterring others in the community from behaving antisocially.

The Information Tribunal considered the question further in *London Borough of Camden v Information Commissioner* (Camden v IC). It was decided that the Council could not pass on details of tenants subject to historic ASBOs to a journalist conducting research. The Tribunal accepted Stanley v Brent, but stated that publication significantly after the judgement would be overly prejudicial to the offender, for example if they were successfully resolving their behavioural problems.

The Tribunal applied the sixth data protection principle. According to this, non-sensitive personal information can be passed to third parties if:

"…necessary for the purposes of legitimate interests pursued by the data controller or by the third…parties to whom the data are disclosed, except where…unwarranted… by reason of prejudice to the rights and freedoms or legitimate interests of the data subject."

This can be applied to the publication of personal details alongside any court judgement. It follows that before publishing such details, landlords should confirm:

1. They have a legitimate aim.
2. The proposed publication is necessary to achieve this.
3. The tenant will not be disproportionately affected.

Simply naming and shaming is unlikely to be considered a legitimate aim. However, it can be safely said that assuring or warning other tenants that a problem is being addressed and deterring its recurrence is.There then follows a balancing act between the landlord's justification for publishing personal details and the prejudice to the tenant. Publication should be considered on a case by case basis and, as a rule of thumb:

a. The older and less severe the case, and the less relevant the personal details are, the less justification for publishing.
b. The more personal information and the greater number of people it is disseminated to, the greater the prejudice to the tenant (and the greater the justification for publishing required).

"The explicit and information-specific (rather than blanket) signposting of an expectation of confidentiality will, however, help to make the engagement of regulation 12(5)(e) less contentious"

In summary, landlords can publish the details of tenants subject to judgements if this will help tackle a wider problem, but only if the tenant's rights have been properly considered beforehand. There is no 'one size fits all' approach and if you have any doubt on whether you can publish, then we will be happy to assist.

Charles Tetlow is a solicitor in Devonshires Housing Management Team. He specialises in data protection and FOIA issues in the housing management context, in particular data protection breaches and requests from tenants for release of information. Charles can be contacted on charles.tetlow@devonshires.co.uk or 020 7880 74211.

Ask the Expert

In this first edition of I-Brief, our resident information law expert is asked to advise a rather agitated Corporate Services Director of a well-known RP.

"A member of staff has accidentally emailed all of our residents the list of names and addresses of our shared ownership applicants including details of their bank accounts and their mortgage accounts. Apparently they intended to send it to the Head of Leasehold but clicked the wrong button. What do we do? Help!"

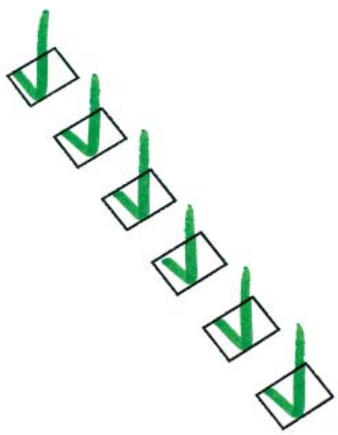
Our Expert says:

Don't panic. These things happen. You would be surprised how many inadvertent breaches of the DPA occur in the social housing sector and elsewhere. Having said that, you need a robust action plan implemented quickly. The Information Commissioner now has powers to fine organisations for data protection breaches and the fines can be eye–watering. However, if we take certain steps we can mitigate the risk of sanctions by the ICO.

Consider the following **Seven Point Plan**:

1. Can the email be recalled? Not particularly useful where people are monitoring their emails, but useful if they only do so occasionally.
2. Send an email to all recipients explaining that the disclosure was inadvertent and asking that they delete the email. Explain that any dealing with the information is prohibited and use of the information may result in legal action or criminal prosecution.
3. Send a letter to residents whose information was disclosed, fully explaining the circumstances of the disclosure and advising them to contact their bank to warn them to be alert to any suspicious transactions.
4. Contact the ICO to advise them of the breach and to confirm the steps being taken to (a) deal with the breach and (b) to avoid the same thing happening in the future. Do not contact the ICO until you have your action plan in place. The ICO will not be impressed by a panicky call at the outset where you have no plan of action.
5. Prepare a press statement – local press loves nothing more than a housing association in trouble and data protection breaches are always newsworthy. The local hack may hope the story gets picked up by the Nationals.
6. Taking disciplinary action against the employee will be unlikely unless the member of staff should not have had access to the list in the first place or has deliberately done this.
7. Revisit your procedures and your email systems to build in technical protections to prevent the same thing happening again. The ICO is very keen on seeing what steps have been taken to prevent a repeat occurrence. If there is a similar breach in the future the ICO will take account of past breaches in assessing whether to impose sanctions.

"The ICO will not be impressed by a panicky call at the outset where you have no plan of action."



Meet our Information Team

Nick Billingham
Partner
020 7880 4272
nick.billingham@devonshires.co.uk

Philip Barden
Partner
020 7880 4280
philip.barden@devonshires.co.uk

Ronnie Tong
Solicitor
020 7880 4335
ronnie.tong@devonshires.co.uk

Elen Storey
Solicitor
020 7880 4389
075 2525 5839
elen.storey@devonshires.co.uk

Charles Tetlow
Solicitor
020 7880 4211
charles.tetlow@devonshires.co.uk

Freephone Information Helpline

Help is at hand

Information Helpline

Devonshires is pleased to announce the launch of our new free Information Helpline. Gain instant access to our lawyers throughout the business day. Get direct legal advice on specific issues and a quick response to an immediate problem.

Information Helpline

0800 051 4212

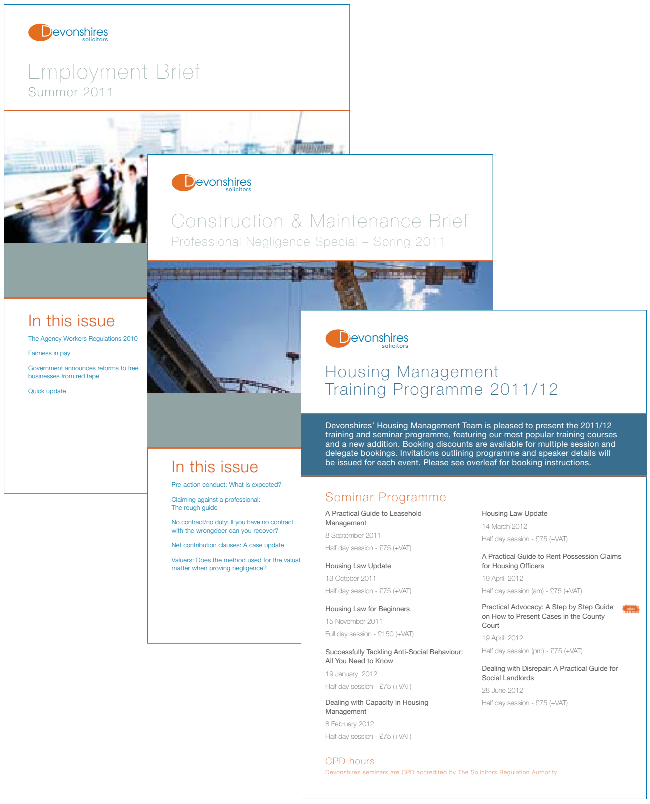
Monday to Friday 9am - 5pm

Legal updates

Devonshires produce a wide range of briefings and legal updates for clients as well as running comprehensive seminar programmes.

If you would like to receive legal updates and seminar invitations please visit our website on the link below.

http://www.devonshires.com/join-mailing-list



Edited by: Nick Billingham
Head Office: 30 Finsbury Circus, London EC2M 7DT
For further copies please contact the Marketing Department on: 020 7628 7576, or email info@devonshires.co.uk or visit www.devonshires.com