A PRACTICAL GUIDE TO IT LAW

3rd edition

Edited by Jeremy Holt and Jeremy Newton

The Chartered Institute for IT
BCS, THE CHARTERED INSTITUTE FOR IT

BCS, The Chartered Institute for IT, is committed to making IT good for society. We use the power of our network to bring about positive, tangible change. We champion the global IT profession and the interests of individuals, engaged in that profession, for the benefit of all.

Exchanging IT expertise and knowledge
The Institute fosters links between experts from industry, academia and business to promote new thinking, education and knowledge sharing.

Supporting practitioners
Through continuing professional development and a series of respected IT qualifications, the Institute seeks to promote professional practice tuned to the demands of business. It provides practical support and information services to its members and volunteer communities around the world.

Setting standards and frameworks
The Institute collaborates with government, industry and relevant bodies to establish good working practices, codes of conduct, skills frameworks and common standards. It also offers a range of consultancy services to employers to help them adopt best practice.

Become a member
Over 70,000 people including students, teachers, professionals and practitioners enjoy the benefits of BCS membership. These include access to an international community, invitations to a roster of local and national events, career development tools and a quarterly thought-leadership magazine. Visit www.bcs.org/membership to find out more.

Further information
BCS, The Chartered Institute for IT,
3 Newbridge Square,
Swindon, SN1 1BY, United Kingdom.
T +44 (0) 1793 417 417
(Monday to Friday, 09:00 to 17:00 UK time)
www.bcs.org/contact
http://shop.bcs.org/
A PRACTICAL GUIDE TO IT LAW
3rd edition

Jeremy Holt and Jeremy Newton (editors)
## CONTENTS

List of figures and tables ix  
Contributors x  
Acknowledgements xiii  
Abbreviations xiv  
Foreword to the 3rd edition xvii

### 1. IT CONTRACTS – Jeremy Holt

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Parts of a contract</td>
<td>1</td>
</tr>
<tr>
<td>Who are you going to call?</td>
<td>2</td>
</tr>
<tr>
<td>Checking out the supplier</td>
<td>3</td>
</tr>
<tr>
<td>Letter of intent</td>
<td>3</td>
</tr>
<tr>
<td>The supplier’s terms</td>
<td>3</td>
</tr>
<tr>
<td>What contracts are there likely to be?</td>
<td>4</td>
</tr>
<tr>
<td>Appendix: main points of an IT contract</td>
<td>11</td>
</tr>
</tbody>
</table>

### 2. CLOUD COMPUTING – Stuart Smith, Mark Poston and Rachel Anderson

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>13</td>
</tr>
<tr>
<td>What is cloud computing?</td>
<td>13</td>
</tr>
<tr>
<td>The evolution of cloud computing</td>
<td>14</td>
</tr>
<tr>
<td>Factors that contributed to the rise of cloud services</td>
<td>14</td>
</tr>
<tr>
<td>Cloud formations</td>
<td>16</td>
</tr>
<tr>
<td>Silver linings</td>
<td>16</td>
</tr>
<tr>
<td>Thunder clouds</td>
<td>18</td>
</tr>
<tr>
<td>Summary</td>
<td>20</td>
</tr>
<tr>
<td>References</td>
<td>20</td>
</tr>
</tbody>
</table>

### 3. CLOUD COMPUTING CONTRACTS – Sam De Silva

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>21</td>
</tr>
<tr>
<td>Pre-contractual steps</td>
<td>22</td>
</tr>
<tr>
<td>Key commercial and legal issues</td>
<td>24</td>
</tr>
<tr>
<td>Summary</td>
<td>35</td>
</tr>
</tbody>
</table>

### 4. INTELLECTUAL PROPERTY LAW FOR COMPUTER USERS – Jennifer Pierce

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>36</td>
</tr>
<tr>
<td>Hardware and intellectual property rights</td>
<td>37</td>
</tr>
<tr>
<td>Software and intellectual property rights</td>
<td>38</td>
</tr>
</tbody>
</table>
Databases and intellectual property rights 40  
Websites and intellectual property rights 41  
Domain names and intellectual property rights 42  
The internet and trade marks 43  
The internet and copyright and database right 45  
Appendix: a basic guide to intellectual property and related rights 45  
Taking advice 50  
Summary 50  

5. CYBER SECURITY – Andy Lucas 51  
Introduction 51  
What is cyber security? 51  
What are the main forms of cyber attack? 57  
What are the risk areas? 60  
What laws govern cyber security? 69  
What practical steps should you consider? 75  
What guides, frameworks and standards are available? 85  
Summary 92  
References 94  

6. GDPR AND DATA PROTECTION: THE LAW – Victoria Hordern 96  
Introduction 96  
What data are covered? 96  
Special categories of personal data 97  
Data protection principles 98  
Rights of individuals 104  
Exemptions 110  
Remedies, enforcement powers and penalties 111  
Summary 115  

7. DATA PROTECTION IN PRACTICE – Andrew Katz, Michaela MacDonald, Tim Astley, Usha Guiness, Jiri Svorc and Chris McCormick 116  
Introduction 116  
Data protection by design and default 116  
What amounts to ‘processing personal data’ under the GDPR? 117  
Creating a ‘record of processing’ 119  
Deciding upon the lawful basis of processing 120  
Drafting data protection policies 124  
Data Protection Impact Assessments 125  
Requests from data subjects 125  
Children’s personal data 127  
Controllers and processors 130  
Sub-processors 133  
Data protection officers 134  
International transfers 135  
Processing data of EU data subjects 138  
Breach notifications 139  
Summary 142
<table>
<thead>
<tr>
<th>8.</th>
<th>IT IN THE WORKPLACE: PROTECTING THE EMPLOYER – Jeremy Holt</th>
<th>143</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Introduction</td>
<td>143</td>
</tr>
<tr>
<td></td>
<td>Computer and email usage policies</td>
<td>143</td>
</tr>
<tr>
<td></td>
<td>Social media</td>
<td>152</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>155</td>
</tr>
<tr>
<td>9.</td>
<td>IT IN THE WORKPLACE: AVOIDING EMPLOYMENT PROBLEMS – Nicola Cordell</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>Health and safety responsibilities</td>
<td>156</td>
</tr>
<tr>
<td></td>
<td>Employment law</td>
<td>161</td>
</tr>
<tr>
<td></td>
<td>Further advice</td>
<td>163</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>163</td>
</tr>
<tr>
<td>10.</td>
<td>OPEN SOURCE SOFTWARE – Andrew Katz and Michaela MacDonald</td>
<td>165</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>165</td>
</tr>
<tr>
<td></td>
<td>What is open source?</td>
<td>165</td>
</tr>
<tr>
<td></td>
<td>Open source and communities</td>
<td>171</td>
</tr>
<tr>
<td></td>
<td>Open source software business models</td>
<td>172</td>
</tr>
<tr>
<td></td>
<td>Businesses as customers of open source</td>
<td>174</td>
</tr>
<tr>
<td></td>
<td>Open source licensing in greater depth</td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>Procuring on-premise open source</td>
<td>185</td>
</tr>
<tr>
<td></td>
<td>Licensing requirements</td>
<td>186</td>
</tr>
<tr>
<td></td>
<td>Open source in the supply chain</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Open source compliance policies and procedures</td>
<td>190</td>
</tr>
<tr>
<td></td>
<td>Open source software: employees and contractors</td>
<td>191</td>
</tr>
<tr>
<td></td>
<td>Open source software and patents</td>
<td>193</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>194</td>
</tr>
<tr>
<td></td>
<td>Further information</td>
<td>195</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>195</td>
</tr>
<tr>
<td>11.</td>
<td>AGILE SOFTWARE DEVELOPMENT– Stewart James</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>The Agile Manifesto</td>
<td>198</td>
</tr>
<tr>
<td></td>
<td>Commercial challenges</td>
<td>201</td>
</tr>
<tr>
<td></td>
<td>Commercial models</td>
<td>207</td>
</tr>
<tr>
<td></td>
<td>Contract drafting</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Template examples</td>
<td>210</td>
</tr>
<tr>
<td></td>
<td>Summary</td>
<td>211</td>
</tr>
<tr>
<td>12.</td>
<td>SETTING UP JOINT VENTURES – Andrew Katz</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td>Joint ventures and IT projects</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td>Establishing a joint venture</td>
<td>214</td>
</tr>
<tr>
<td></td>
<td>Structure of a joint venture</td>
<td>216</td>
</tr>
<tr>
<td></td>
<td>The operating agreement</td>
<td>222</td>
</tr>
</tbody>
</table>
LIST OF FIGURES AND TABLES

Figure 11.1  Comparison of software development methodologies  199
Figure 11.2  Cone of uncertainty  202

Table 3.1    Key contractual issues with SaaS contracts  30
Table 10.1   Comparison of typical open source licences with typical proprietary software licences  167
Table 10.2   Summary of the key provisions of popular open source software licences  176
Table 12.1   Factors to consider when forming an entity  217
Table 13.1   Negotiation  229
Table 13.2   Expert determination  230
Table 13.3   Litigation  232
Table 13.4   Arbitration  234
Table 13.5   Mediation  237
**CONTRIBUTORS**

**Rachel Anderson** is an in-house paralegal at Natixis Investment Managers. She was previously a paralegal at software company Beamery, and at Algomi, a fin-tech company that provides cloud-based technology to bond market participants and where she worked alongside contributor Stuart Smith. Prior to working as a paralegal, Rachel read law (LLB) at the University of Manchester, where she developed a particular interest in commercial and intellectual property law.

**Tim Astley** is a partner in the Moorcrofts technology department. He is a solicitor with postgraduate qualifications from both Strathclyde University and Queen Mary, University of London in technology and communications law. He has worked on private, public and regulated sector transactions. He has extensive cloud computing contract experience, and has negotiated high-value complex agreements in many jurisdictions around the world. His practice involves providing specialist advice on data protection and open source compliance.

**Nicola Cordell** is a specialist occupational physician, researcher and educator, passionate about developing further understanding of employee health. She is the managing director of a social enterprise, Cordell Health Ltd. The organisation provides workplace health and wellbeing services, such as specialist advice on health and safety and employment issues relating to health across sectors, including the science and technology sector. In her education role, she develops training, in partnership with other professional groups including legal, IT and accountancy specialists, that is delivered to organisations and occupational health professionals, ensuring that advances in the knowledge base in this area are widely known.

**Sam De Silva** FBCS, CITP is a partner at CMS Cameron McKenna Nabarro Olswang LLP and specialises in complex and strategic IT and telecommunication projects. Sam is the Law Society’s representative on the European Commission’s Expert Group on Cloud Computing Contracts. Sam was elected to the Trustee Board of BCS in 2019 and has been on the Council of BCS since 2016 (vice-chair 2016–2017). In October 2020 Sam was elected as chair of BCS Law Specialist Group. Sam has also recently been appointed as the inaugural chair of the Diversity and Inclusion Advisory Board of the Society of Computers and Law.

**Sara Ellacott** is EMEA Assistant General Counsel for Litigation at Oracle Corporation. Sara advises on issues arising in the IT sector and has experience of a wide range of dispute resolution procedures, including negotiated settlements, High Court litigation, arbitration and mediation. Sara speaks regularly on issues relating to legal risk and dispute management.
Usha Guness is a dual qualified barrister and solicitor. She has over fifteen years’ experience in the commercial and technology field, which includes private practice as well as international experience working for several companies including a major global telecommunications company. She has a wide breadth of experience in advising, drafting and negotiating commercial and technology contracts as well as regulatory and compliance matters. She holds a Masters and recently obtained a certificate in US Copyright Law from the Berkman Center at Harvard University.

Jeremy Holt is the former senior partner of Clark Holt Commercial Solicitors (www.clarkholt.com). He has specialised in IT and e-commerce law for over 30 years. In 2003 Jeremy helped set up in Swindon the first museum in the country dedicated to the history of computing. He has co-authored two other books on IT law.

Victoria Hordern is a partner at London law firm Bates Wells, where she is Head of Data Privacy. She advises on a wide range of data privacy issues, including all types of GDPR-related obligations (from DPIAs to responses to data security breaches), as well as online privacy issues connected with the e-privacy legal framework. Her experience includes UK, pan-European and global privacy matters for commercial businesses and non-profits/charities. Victoria advises on international data transfers, whistleblowing, outsourcing, cookie compliance and employee monitoring. She holds the International Association of Privacy Professionals’ CIPP/E and CIPT certifications and is a member of the IAPP’s Privacy Faculty providing training on data privacy.

Stewart James is a director and the founder of Agillex, an alternative professional services consultancy that was established to work collaboratively with clients and enable the realisation of outcomes instead of imposing solutions. Previously, Stewart, a lawyer with over 20 years’ experience, was a partner at DLA Piper LLP.

Andrew Katz is CEO and partner at Moorcrofts LLP, a niche corporate and technology legal practice based in Marlow, Buckinghamshire, where he heads the technology team. Andrew qualified as a barrister and subsequently re-qualified (and now practises) as a solicitor in England and Wales. He is also a solicitor (non-practising) in Ireland. He is a founder editor of the International Free and Open Source Software Law Review (now the Journal of Open Law, Technology and Society), a fellow of the Free Software Foundation Europe and a fellow of the Open Forum Academy. He is also founder and CEO of Orcro Ltd, a consultancy specialising in compliance issues, with special emphasis on open source supply chain licence compliance.

Andy Lucas is Head of the Technology, Media and Telecommunications department at Dentons. Prior to becoming a lawyer, he was a software programmer and project manager. During his 20-plus years in the legal profession, Andy has specialised in advising government and private sector companies on their technology implementations and cybersecurity. As well as advising clients, Andy lectures on a wide variety of technology law issues including blockchain, artificial intelligence and augmented reality.

Michaela MacDonald is a lecturer at Queen Mary University and Beijing University of Posts and Telecommunications. She teaches Interactive Entertainment Law, AI, Robotics and the Law, Cybersecurity Law and Product Development. Michaela’s main research interests are in the legal, regulatory and societal effects of disruptive technologies. She has been involved in projects exploring the legal and regulatory implications of cloud computing, and, most recently, investigating the legality of smart contracts. Michaela
is also working at Moorcrofts LLP as a consultant, collaborating on projects that have focused on the legality of data and text mining activities, open source licences classification and contract automation.

Chris McCormick is an experienced contracts manager, having previously worked at a large technology company in the Thames Valley handling their contract administration. In addition to his legal and process experience, he has particular interest in SalesForce implementation and is currently working with a number of Moorcrofts’ clients to provide contracts management services and also help to develop the clients’ processes around SalesForce. Chris has completed the LPC and is in the process of qualifying as a solicitor. Prior to his career in law, Chris worked as a freelance IT consultant specialising in enterprise storage and storage area networks.

Jeremy Newton is a director of Technology Law Alliance, a specialist IT/outsourcing law firm based in London. He has over 25 years’ experience of IT and outsourcing contracts, both in private practice and as an in-house lawyer within the IT sector, and is ranked as one of the leading IT lawyers in London by the current Chambers directory. Jeremy advises a wide variety of IT businesses on their contracts, ranging from start-ups through to Tier 1 global outsourcing service providers. He also advises customer organisations including financial institutions, housebuilders, charities and public sector bodies. Jeremy has written and lectured widely on IT law and contracts, outsourcing, data protection and e-commerce matters, and is a past secretary of the Financial Services Specialist Group of BCS.

Jennifer Pierce is a partner in the City law firm, McCarthy Denning, where she specialises in intellectual property and information technology. This includes strategies for protection of software and hardware, including patenting (where possible), the use of open source, Internet of Things and work on the overlap with mechanical engineering as well as issues arising from the internet. Her clients range from multinational companies to research institutes to start-ups. She is ranked as a Global Leader by Intellectual Asset Management and is a past president of the Licensing Executives Society Britain & Ireland, the influential IP commercialisation society.

Mark Poston is Commercial Manager at Tempora, a software company that provides time tracking, cost and profitability analysis solutions via the cloud to a wide range of market sectors in the UK, US and Asia. Mark graduated from the University of Brighton in 2014 (BSc Computer Science) and 2015 (MSc Marketing & Behaviour Science).

Stuart Smith has run the legal operations at both Beamery and Algomi, each providers of B2B cloud services (respectively in the recruit-tech and fin-tech sectors). Previously, Stuart worked in private practice law firms including Clark Holt, Osborne Clarke and Technology Law Alliance. He has had long-standing involvement in his family business, Tempora, a provider of cloud-based time-tracking services.

Jiri Svorc has participated in advising businesses as well as public sector organisations on technology, intellectual property and complex commercial law matters, as well as on personal data protection, cyber security and open source licensing and compliance. Most notably, Jiri has participated in cross-border technology transfers, and advised leading global technology companies as well as technology disruptors. Jiri has obtained LLM from Queen Mary, University of London and has worked with a number of law firms in the UK and EU, as well as with DG Connect of the European Commission.
The authors wish to acknowledge the contributions made by the following:

Jane Bright
Julieta De Silva
Leonardo De Silva
Stella De Silva
Lizzy Gagan
Dawn Holt
David Hudson
Nathan Hudson
Nia Hudson
George Johnson
Lucy Katz
Andrew Kite
Paul Langford
Antonia Newell
Lucy Newton
Arthur Smith
Christopher Smith
Theodore Smith
Wilbur Smith
Heather Stewart
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGPL</td>
<td>Affero GPL</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider/Provision</td>
</tr>
<tr>
<td>AUP</td>
<td>Agile Unified Process</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BCR</td>
<td>Binding Corporate Rule (GDPR)</td>
</tr>
<tr>
<td>BSD</td>
<td>Berkeley Software Distribution</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CAA</td>
<td>Copyright Assignment Agreement</td>
</tr>
<tr>
<td>CC</td>
<td>Creative Commons</td>
</tr>
<tr>
<td>CCS</td>
<td>Crown Commercial Services</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CEO</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>CIF</td>
<td>Cloud Industry Forum</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CISQ</td>
<td>Consortium for IT Software Quality</td>
</tr>
<tr>
<td>CLA</td>
<td>Contributor Licence Agreement</td>
</tr>
<tr>
<td>CPR</td>
<td>Civil Procedure Rules</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>CSCC</td>
<td>Cloud Standards Customer Council</td>
</tr>
<tr>
<td>CSO</td>
<td>Chief Security Officer</td>
</tr>
<tr>
<td>CTO</td>
<td>Chief Technology/Technical Officer</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Processing Agreement</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>DPL</td>
<td>Data Protection Lead</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>DSDM</td>
<td>Dynamic Systems Development Method</td>
</tr>
<tr>
<td>DSE</td>
<td>Display Screen Equipment</td>
</tr>
</tbody>
</table>
ABBREVIATIONS

DSP  Digital Service Provider (NIS Directive)
EEA  European Economic Area
EEIG  European Economic Interest Grouping
ENISA  European Union Agency for Network and Information Security
ERP  Enterprise Resource Planning
EU  European Union
FDD  Feature-Driven Development
FLOSS  Free, Libre and Open Source Software
FOSS  Free and Open Source Software
FSF  Free Software Foundation
GDPR  General Data Protection Regulation 2016/679
GPL  General Public License
HSE  Health and Safety Executive
IaaS  Infrastructure as a Service
IASME  Information Assurance for Small and Medium Enterprises
ICO  Information Commissioner’s Office
ICS  Industrial Control System
IEC  International Electrotechnical Commission
IEEE  Institute of Electrical and Electronics Engineers
IoT  Internet of Things
IP  Intellectual Property or Internet Protocol (address)
ISMS  Information Security Management System
ISO  International Organization for Standardization
ISP  Internet Service Provider
ISS  Information Society Service
IT  Information Technology
ITU  International Telecommunication Union
LGPL  Library/Lesser General Public License
LIA  Legitimate Interest Assessment
LLC  Limited Liability Corporation
LLP  Limited Liability Partnership
MAC  Media Access Control
MFA  Multi-Factor Authentication
MIT  Massachusetts Institute of Technology
MitM  Man in the Middle (attack)
MPL  Mozilla Public License
MVP  Minimum Viable Product
NA  Network Administrator
NCSC  National Cyber Security Centre
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NDA</td>
<td>Non-Disclosure Agreement</td>
</tr>
<tr>
<td>NHS</td>
<td>National Health Service</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Systems (Directive/Regulation)</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology (USA)</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OES</td>
<td>Operator of Essential Services (NIS Directive)</td>
</tr>
<tr>
<td>OFT</td>
<td>Office of Fair Trading</td>
</tr>
<tr>
<td>OIN</td>
<td>Open Invention Network</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Source Initiative</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PECRs</td>
<td>Privacy and Electronic Communications Regulations 2003</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>RDSP</td>
<td>Relevant Digital Service Provider</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-frequency Identification</td>
</tr>
<tr>
<td>SA</td>
<td>Sharealike</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAFe</td>
<td>Scaled Agile Framework</td>
</tr>
<tr>
<td>SAR</td>
<td>Subject Access Request</td>
</tr>
<tr>
<td>SCC</td>
<td>Standard Contractual Clause</td>
</tr>
<tr>
<td>SEQOHS</td>
<td>Safe and Effective Quality Occupational Health Service</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Instrumented Systems</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid-state Drive</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>T&amp;M</td>
<td>Time and Materials</td>
</tr>
<tr>
<td>TCC</td>
<td>Technology and Construction Court</td>
</tr>
<tr>
<td>ToS</td>
<td>Terms of Service</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>VAT</td>
<td>Value Added Tax</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>XP</td>
<td>Extreme Programming</td>
</tr>
</tbody>
</table>
This book is a practical guide to IT law. The authors felt the law in England in this area should be summarised in a way that is easy to understand. Things have changed so much and so quickly since the last edition that it was felt that the book should be updated to reflect these changes.

The book is not designed to be read from cover to cover. Readers can dip into the various self-contained chapters to find the answers that they seek. It provides practical advice on the appropriate steps that should be taken.

We hope that it will be a valuable guide to IT professionals as well as being of interest to managers, legal practitioners and students.

Jeremy Holt and Jeremy Newton
This chapter outlines the contents of a contract and lists the matters that should be covered by different types of contract. If you do not have time to read the rest of the chapter, the appendix lists the main points that you should consider.

INTRODUCTION

Pity the unfortunate manager. It has been bad enough trying to get the computer project organised. Now, possibly at the last moment, the contracts have arrived, some with print small enough to make the reader go blind. The manager suspects (rightly) that these contracts are one-sided in favour of the supplier, but knows that the project will only proceed if those contracts (or something similar) are signed. How does the manager work out what needs to be done and from whom advice can be obtained? This chapter provides a practical framework of help in this situation. If you are looking for an academic guide to computer contracts, you will need to look elsewhere.

PARTS OF A CONTRACT

The first point to consider is the form that contracts normally take. At its simplest, a contract consists of:

1. the date on which the contract was entered into;
2. the names and addresses of those entering into the contract;
3. a short description of what the contract is about (generally entitled ‘Background’, ‘Recitals’ or even, regrettably, ‘Whereas’);
4. definitions of terms used in the contract;
5. what the supplier is going to do for you;
6. what you must do for the supplier;
7. what you must pay the supplier.

Do not forget we are engaged in contract first aid here. If all else fails, concentrate on points (5) and (7), that is, what the supplier is going to do for you and what you are expected to pay. Standard terms that are not specific to this individual contract (what lawyers call ‘boilerplate’) are generally grouped together at the end of the contract.
IMPORTANT BOILERPLATE TERMS

These are some of the more important boilerplate clauses you may come across.

**Force majeure** – this says that neither party shall be liable for any failure to perform the contract because of circumstances beyond its control such as an Act of God, fire, flood and so on. This is more likely to be invoked by the supplier than the client because this clause effectively absolves the supplier from responsibility.

**Entire agreement** – this says that the entire agreement between the parties is set out in the written contract and so no other previous representations by the supplier may be relied upon by the client. This is a reasonable principle, but the client must make sure that the contract deals with all the important points.

**Notices** – this specifies the agreed means of sending formal notices. Normally, this requires a notice to be in writing, to avoid issues surrounding an oral notice (i.e. proving delivery and contents). However, what qualifies as ‘writing’ may differ from contract to contract. For example, some clauses may expressly state that a notice is not valid if sent by email. A notices clause may also specify the personal details of a party on whom a notice must be served to ensure it comes to the attention of the appropriate party.

**Dispute resolution** – it is sensible to agree an alternative dispute resolution procedure (such as mediation) that must be carried out before any dispute is referred to the courts or to arbitration.

**Governing law and jurisdiction** – ideally this should be English law enforced in the English courts. An alternative is to agree arbitration, but as this happens behind closed doors then the supplier may worry less about bad publicity.

WHO ARE YOU GOING TO CALL?

You are not going to be able to do all this on your own. You are going to need professional advice. Computer law is a specialist area, and a rapidly changing one (it did not even exist as a field of legal practice 30 years ago) and the correct advice from a lawyer experienced in this field can save a great deal of trouble later. The function of a good lawyer is to assess risk, help the client to understand the level of risk and then reduce it.

There are two directories of lawyers that you might like to consult: *Chambers’ Guide to the Legal Profession* and *The Legal 500*. New versions are published each year, and each has sections on lawyers who specialise in computer law (sometimes called ‘information technology law’). These two books can generally be found in the reference section of a public library, and can also be searched without charge on the web. Alternatively, you can ring the Law Society or the Society for Computers and Law for suggestions of lawyers who work in this field and who could help you.
CHECKING OUT THE SUPPLIER

It may seem like an obvious point but make sure that you know who you are dealing with. This will mean, at least, doing a company search. A credit check would do no harm. As the Army maxim has it, ‘time spent on reconnaissance is seldom wasted’. If you discover that the supplier company was set up last year and has an issued capital of £1, you may like to consider asking for a guarantee of the contract from a more substantial body.

Business is not all about making rational decisions on paper. Do you get good vibes from the supplier? On small things, do they do what they say that they will do? If, for whatever reason, you do not trust them, do not go ahead with the contract under any circumstances, as this will only lead to worry and tears later.

LETTER OF INTENT

As the supplier may need to start work on your project before contracts are signed, and because the negotiation and agreement of the contract terms may take a little while, the supplier may ask for a letter of intent from you. Alternatively, you may like to suggest one so that you are not pressurised into signing the contracts before you have reviewed them properly.

A letter of intent is no more than written confirmation from you of your intention to enter into a contract with the supplier. What is critical, however, is that your letter of intent states that the letter is not intended to be contractually binding. Otherwise, you may unwittingly enter into a contract earlier than you intended.

Where there is a non-binding letter of intent and the supplier, at your request and to save time, starts work on the project, it is reasonable for the supplier to ask to be paid for this initial work carried out regardless of whether the project proceeds or not. There are two important matters to agree here. The first is the rate for the work carried out (e.g. a daily rate). Work normally starts under a letter of intent on a time and materials basis; the definitive contract may include a fixed price for a specified deliverable. The second is an overall cap on the total amount of payment to the supplier for this work. This obligation to pay the supplier should be contractually binding (unlike the rest of the letter of intent).

THE SUPPLIER’S TERMS

It is a good idea to ask for the supplier’s proposed terms at as early a stage as possible. Do not wait until you have told them that they have been awarded the contract. There is of course no obligation on you to accept that you will purchase a new computer system on the basis of the supplier’s terms. You could propose your own terms entirely – this is certainly an approach taken by large organisations with extensive experience of computer contracts. However, it is generally better to use the supplier’s contract terms (unless they are completely unreasonable) as a starting point and amend them to your satisfaction.
If a particular point is important to you, make sure that you get it in writing from the supplier. It may well be that a critical aspect is not dealt with in the supplier’s draft contract at all. If so, you must, for evidence’s sake, get it in writing from the supplier. An ordinary letter from the supplier is sufficient provided that it is either referred to in the main contract or included as a schedule or as an attachment. If the supplier drags their heels and, despite repeated requests from you, refuses to confirm a point in writing, you should write to the supplier saying that you are only entering into the main contract on the basis that this point is agreed. If the matter ever goes to court, the production of your letter will be of great assistance to your case.

WHAT CONTRACTS ARE THERE LIKELY TO BE?

Any computer system will require the purchase, licence and maintenance of hardware (the server, PCs, printers, etc.), software (the application software and the operating system software) and services (such as support and maintenance). Previously, the emphasis was very much on the hardware, but nowadays the focus is much more on the software and services. Nevertheless, this chapter discusses all the contracts you are likely to need.

Generally, it is better to decide upon the software first and then to choose the appropriate hardware. Alternatively, you may enter into a contract for consultancy services first, to assist with this process. Consequently, this chapter will deal with such contracts in this order.

Contracts for consultancy services

Long before the order for a new system is placed, the client may enter into a consultancy contract, perhaps relating to a feasibility study, analysing requirements, recommending a system to meet those requirements, helping to select the appropriate suppliers, or assisting with preparation of an invitation to tender. A large part of the work carried out in the computer industry is under consultancy contracts. The client may need help on a one-off basis or require skills that do not exist within the client’s workforce, so need an outside consultant to carry out the work. Sometimes the consultancy arrangement is dealt with by means of an exchange of letters; a formal consultancy agreement, however, is a better option for both parties.

- **Defining the deliverables** – one of the most important issues that must be dealt with in such a contract is a detailed description of what the consultant is expected to do. If the description is loose or inexact, this can give rise to differences between what the client is expecting to receive and what the consultant is expecting to deliver – which can, predictably, lead to disputes. So, defining the nature and quality of the deliverable is particularly important.

- **Payment arrangements** – the payment to the consultant by the client may be on a time and materials, fixed price or estimated maximum price basis. It is an aspect of consultancy that the amount of work required will be uncertain. The disadvantage of a fixed price payment mechanism (as with any other contract) is that the consultant will inevitably include a contingency element in the price quoted. If the consultancy can be broken down into a series of stages, payment against milestones will allow each party to gauge how the work is going.
• **Copyright** – copyright will almost always be an issue. Broadly speaking, there is a simple choice as to how the parties deal with ownership of copyright in the consultant’s work. Either the consultant can assign to the client all intellectual property rights in whatever is produced (provided that the consultant has been fully paid) or the consultant can grant a perpetual licence to the client to use such intellectual property rights for the purposes of the client’s business (see Chapter 4 for more details). It is important to note that if there is no agreement with a consultant about copyright, the client does not automatically get ownership of such copyright. It stays with the consultant (although there may also be an implied licence for use of the copyright by the client).

• **Confidentiality** – it goes almost without saying that the consultant should be obliged to keep confidential any information given by the client about its business. The problem is that once a consultant has carried out an assignment for one client in an industry, the consultant may be ideally placed to carry out assignments for other clients within that same industry. Sometimes, therefore, clients go further and stipulate in the contract that not only must their own information be kept confidential, but the consultant must agree not to carry out projects for the client’s competitors for a period (perhaps a year) after the work is completed.

• **Insurance** – in order to provide peace of mind to the client, the client may require the consultant to take out professional indemnity insurance. This is still relatively inexpensive as, in practice, it is rare for claims to be made under such policies.

• **Key personnel** – the client will want to know the identity of the staff who the consultant will be using to carry out the work. It is normal for the client to be able to veto any staff members of whom they disapprove for whatever reason.

• **Termination** – the client will want to retain the right to terminate the consultancy contract if the consultant is guilty of serious misconduct or any other conduct likely to bring the client into disrepute.

### Contracts for software licences

At its simplest, any contract for software should allow you to use the software in the way that you envisaged without the risk that anyone can come along later and say either that you cannot use it any more or that you have to pay more money. It follows, therefore, that one of the first checks you should do is to confirm that the software supplier either owns the copyright in the software or has the right to license it to you. It is a feature of the computer industry that software is often licensed to end users by organisations other than the actual owner (for example it may be sub-licensed by a distributor or channel partner). You should not put up with oblique answers to your demand for evidence that the supplier can license the software to you. They should be able to produce it immediately.

At this point you may wonder why a licence agreement is necessary at all; why can the supplier not simply sell you the software? The supplier is not actually selling you ownership of the software because they would like to continue to license it to other people. The licence is only a permit for you to use the software for your own purposes.

This leads onto the next important point. You must check in the licence agreement to whom the software is licensed and for what purpose. Is the software to be licensed...
to your particular company or can it be used by the whole of your group (in which case the software supplier will want more money)? Alternatively, is the software to be restricted to a limited number of users and, if more than that number use it, then do you have to pay an additional licence fee? This is one of the oldest tricks in the software supplier’s book. They allow the client to sign up for a very limited number of users and then the supplier makes a considerable profit from the additional users that will almost inevitably be required by the client later. The supplier, of course, responds that this simply reflects the extra use (and, as a result, commercial benefit) that the client is making of the software.

It is also possible that, at some time in the future, the client may want to outsource its computer operations. Consequently, provision for the transfer of the licence from the client to an outsourcing company should be made in the original software licence agreement.

Additionally, make sure that the procedure for acceptance testing is known and agreed. If this has not been sorted out in the contract, how are you going to stop a bad system from being installed? In the past, the test data were generally supplied by the client; nowadays it is more acceptable for it to be provided by the supplier.

Contracts for software maintenance

No software of any complexity is ever free from errors. The older the system, the more likely that it will need maintenance. Furthermore, if a system is installed in a rush (e.g. to meet a particular deadline), then it is likely not to have been tested properly so may require more attention after it has been installed. In some ways, future charges for maintenance are the icing on the cake for software developers. If they can generate sufficiently wide sales of the software, then support fees can be guaranteed for years to come. It is important for managers to be aware of this as three-quarters of a budget for software may be for future software maintenance. The client is well advised to check how wide the maintenance supplier’s client base is (the wider the better) and to look at the offices from which the supplier will be providing the support (and how many people will be providing such support). The maintenance contract will almost certainly be prepared by the supplier. Some of the most common provisions are discussed below.

- **Charging arrangements** – sometimes the cost of the software licence is bundled with the first year’s maintenance charges. One interesting point is from when the support charges should run. Some clients argue that they should start from the end of the warranty period for the software. However, it is now generally accepted that they should begin from acceptance of the system, as warranty and support are separate matters.

- **Scope of maintenance services** – maintenance or support will normally cover the investigation by the supplier of errors in the system reported by the client as well as updated documentation and telephone or, more frequently nowadays, online advice. It will, in most cases, cover updates to the software (but not necessarily new versions of the software). The client may want to categorise different kinds of problems into those that could be critical for its business and those that are no more than an irritation and could be dealt with next time a new version of the software comes out. The supplier’s response time will be different depending on the severity of the problem. The supplier will not normally commit to a fix within a particular period – only that they will start to fix it within a particular time.
• **Length of maintenance** – make sure that you get the supplier to agree to supply support and maintenance for the products purchased for a decent length of time, for example five years. You do not want the supplier cancelling support after a couple of years just when your new system is working well. Note that you do not have to commit to take the support and maintenance for five years – ideally your commitment should be on a year-by-year basis. It is just that the supplier agrees to make the support available to you for at least five years if you want it.

• **Exclusions from scope** – the maintenance supplier will also be keen to list in the contract what maintenance does not cover. Most of these exceptions are reasonable. They generally include problems arising from changes to the software made by people other than the supplier, incorrect use of the software by the client, or events beyond the control of the maintenance supplier such as hardware failure, fluctuation of electrical supplies or accidents. Normally, the maintenance supplier will still seek to help the client where the exceptions apply (indeed there should be a contractual obligation to do so). However, the supplier may want to make an additional charge for such work and will not guarantee any particular recovery time. From the supplier’s point of view, it becomes difficult to manage support if the client base is using several different versions of the software. Consequently, the supplier normally restricts support to the latest two versions of the software and will refuse to support earlier versions.

• **Charge increases** – the client will want to ensure that the maintenance charges will not rocket up. One means of doing this is to tie the maintenance charges to a percentage of the list price of the software (e.g. 10–15 per cent) but, of course, the supplier has control over the list price. Alternatively, any increase in maintenance charges can be tied to a recognised index. Clients sometimes suggest the Consumer Price Index. However, suppliers (who know that increases in salaries are generally greater than increases in retail prices) prefer to tie them to an earnings index. There is some logic in this, as the bulk of the supplier’s expenses are salaries.

• **Payment arrangements** – payment is almost invariably made three to six months in advance. This is so that if the supplier goes into liquidation the client will not have overpaid very much and the client can also swiftly withhold the payment of maintenance charges if there is a problem with the service provided.

• **Termination** – it is important for the client to look at the termination clauses of the contract offered by the supplier. The client will want to know how much notice they have to give to end the maintenance contract. This is often three or six months. It is a good idea for the client to ask the supplier to commit on its part to supply maintenance (if the client wants it) for the potential life of the software (e.g. five years).

**Contracts for software development**

Software will often need to be customised for the client by the supplier. However, this is really only a tinkering with the main programs. In certain circumstances, it may be necessary for the client to commission new software because there is no existing software that meets the client’s needs.

Contracts for software development are complex and it is wise for the client to seek professional advice both about the specification for the software and the contract under
which the software will be written. This is all the more important because software development projects have a reputation for taking longer, and costing more, than originally forecast. Consequently, background research by the client into the proposed supplier is particularly worthwhile. Pricing for the project will be either for a fixed price or for time and materials. Payments will normally be made conditional upon project milestones being reached. The client should seek to ensure the quality of the software product delivered by the supplier by requiring acceptance tests of the software and a warranty from the supplier that the product will be in accordance with the agreed specification.

A thorny question is whether the client should own the copyright in the software program produced. At first glance, it might be thought that this should obviously belong to the client who has paid for it. However, the client only needs to use the software, not to own or develop it. It may benefit the client if the supplier has an incentive to carry out further development of the software program and license it to other clients; the original client does not then pay the total cost of all the subsequent fixes and has the benefit of the faults reported by other users. However, if the supplier becomes insolvent, then the client needs access to the source code of the software in order to maintain it. For this reason, the client should require the supplier to put a copy of such source code in escrow with an independent third party so that it is available if required. The supplier will normally provide a warranty that defects in the software reported within a particular length of time after the start of its use will be rectified. This is frequently 90 days after acceptance of the software by the client.

**Contracts for hardware purchase**

Since computer hardware is so much more reliable than it used to be, contracts for the supply of hardware are not generally contentious. A hardware purchase contract requires the following details:

- a detailed description of the hardware (this is likely to be in a schedule);
- a warranty about the quality of hardware (normally this warranty applies for a year after acceptance of the hardware by the client);
- delivery dates;
- price;
- acceptance testing;
- future maintenance;
- training.

Problems can arise if the hardware is not large enough for anticipated demand, and with the integration of hardware (such as servers and printers) that may have been supplied by different suppliers.

In many cases the cost of the hardware is not a large percentage of the total system cost. As profit margins on hardware are relatively low, the software supplier may be relaxed about whether the client obtains the hardware from the software supplier or
from a third-party supplier. It is always worth asking the software supplier to quote for supplying the hardware as they may have better bargaining power than you would have on your own.

At the end of the day, the two most important matters in a contract for hardware are to check that there is an exact description of what you are buying and that there is an obligation on the supplier to repair or replace it if it does not work properly.

**Contracts for hardware maintenance**

Hardware maintenance is more of a commodity than software maintenance and there are likely to be more suppliers for the maintenance of hardware (and so prices are keener). There are two different types of hardware maintenance: preventive maintenance and corrective maintenance. Preventive maintenance covers the regular testing of the hardware (e.g. once every six months) before any problem is reported. Corrective maintenance deals with faults as and when they arise, normally in response to a service call from the client.

With corrective maintenance, the key element is the response time – how quickly will the supplier start to respond to the problem once it is reported? This is generally within a fixed number of working hours. For example, an engineer may have to arrive at the site no more than eight working hours after the problem has been reported by the client. This does not mean that the engineer will solve the problem within eight hours – merely that a start will be made to try to solve it. Sometimes online diagnosis is used: the client’s hardware is linked by telecommunications to the supplier who can solve the fault at a distance. (The impetus for online diagnosis came from the US, where the distances were so great it was often not practicable to send an engineer in person.)

Payment for hardware maintenance is generally made in advance on a monthly or quarterly basis. Other points that will normally be covered in a hardware maintenance contract include a right for the supplier to:

- make an additional charge for frivolous or unnecessary call outs;
- increase the charges from time to time, perhaps in accordance with a recognised index (such as the Consumer Price Index);
- refuse to cover equipment that is more than five years old or is past its reasonable working life.

The client will be under an obligation to:

- pay for corrections that are not caused by the equipment itself (e.g. faults arising from electrical fluctuations);
- notify the supplier of problems promptly after they arise (so that time does not make them worse);
- allow the supplier reasonable access to the equipment.
Service level agreements

Service level agreements (SLAs) are critical to the computer industry, but they are rarely fully understood. Under an SLA, a supplier undertakes to supply a service to a client at a particular level.

Perhaps because so few lawyers have a reasonable working knowledge of the computer industry, SLAs are often drawn up by the participants without legal advice.

A service level agreement should cover:

- the service required (i.e. what the client wants and what the supplier is prepared to commit to supply);
- quality standards (i.e. the standards or levels the supplier must achieve), such as host/terminal response times, batch processing times, ‘uptime’, or processor availability, by specifying what? when? how? and by whom?
- deliverables (e.g. regular reports);
- the consequences of failing to meet service procedures or standards (e.g. compensation in the form of service credits);
- procedures for the client to monitor performance of obligations by the supplier;
- procedures for change control (i.e. changing part of the service that is being provided by the supplier under the agreement);
- terms dealing with access to, and security of, the client’s site and data;
- procedures for disaster recovery (either upon a system failure or following a catastrophe);
- the agreed frequency of meetings between the client and the supplier to review the supplier’s performance of the agreement, properly minuted with subsequent action plans and awards of priority.

Ideally, an SLA should be a self-enforcing agreement within a continuing relationship. There should be no need for either side to litigate and changes required should be dealt with through a change control procedure. For example, a clause may specify that any additional features requested by the client would require an extra cost to be paid to the supplier, and for this to be confirmed in writing by both parties. In some ways the process of creating the SLA is as valuable as the agreement itself.

What form should a service level agreement take?

SLAs can be between different businesses or between different parts of the same organisation (such as the IT department and its users). Facilities management agreements, software maintenance agreements and managed data network agreements are all examples of SLAs. Alternatively, the SLA may be one aspect of a larger agreement for services, that is, it may be the schedule that stipulates how well the services have to be provided and what happens if the supplier does not provide this.

At its weakest, an SLA may be a simple oral understanding, documented by an exchange of letters. The best form is a formal legal agreement with the technical procedures and specifications annexed as separate schedules.
What happens if the terms of a service level agreement are broken?

If the breach is fundamental, the party not in breach will be entitled to terminate the agreement and sue for the loss suffered as a result of the breach. In other circumstances there will be a system for measuring the breach and apportioning costs. These systems range from an event-based system (i.e. if ... then ...) to a more sophisticated system of ‘failure points’ (i.e. if there are more than five examples of ... then ...). The functions of such compensation systems vary from simply drawing attention to a problem to compensation for loss. Compensation for loss is difficult to quantify and, if it is excessive, will be unenforceable by a court. In practice, the right to withhold payment is a valuable weapon. The end (or slowing down) of payments by the client into the supplier’s accounts department is likely to put pressure on the supplier.

Escalation clauses are undervalued and should be more widely used. These provide for a problem to be escalated up the various tiers of management on both sides if it cannot initially be resolved. Even the best SLA does not last for ever and there must be a procedure for orderly termination and (if necessary) migration from the supplier’s system to another system. The failure to include such clauses was a frequent weakness of early SLAs. Migration is critically important in relation to facilities management contracts and, as a rule of thumb, a year is generally allowed for this. The supplier should also be required to provide all reasonable assistance to the client with the migration to another system.

Contracts relating to cloud computing

Cloud computing is sometimes called software as a service. It appears likely to continue to revolutionise the computer industry over the next few years. For a description of what cloud computing is and the contracts that you are likely to need, see Chapters 2 and 3.

Contracts relating to Agile computing

Agile is a particular form of software development that uses short iterations of effort to produce incremental results. This differs from the sequential or ‘waterfall’ approach to development, which requires a detailed description of the subject matter of the contract to be established at or prior to the start of the project. Agile methodologies use a different cultural approach to the development of software, with the expectation of greater participation by the customer. Consequently, Agile requires an alternative form of contract. The use of Agile and the development of contracts using Agile methodologies is described in greater detail in Chapter 11.

APPENDIX: MAIN POINTS OF AN IT CONTRACT

Read this on its own if you do not have enough time to read the rest of this chapter. But read it carefully.

- Make sure that you know exactly what you want and what is achievable, because if you do not know then you are not going to get the contract right. Among the most common causes of computer project failure are unclear client requirements and unrealistic client expectations.
• Make sure that all the prospective suppliers sign a confidentiality agreement with you. If you are going to give them a detailed functional specification of what you want and information about your business, you do not want there to be any question of that confidential information being obtained by your competitors.

• Beware of falling into the trap of entering into a contract before you intend to. There are no legal formalities in the UK about entering into a computer contract, so make sure that all pre-contract correspondence is headed 'subject to contract'. If you leave discussions about a written contract incomplete (e.g. lots of draft contracts sent between you and the supplier but nothing ever signed), then a court is likely to take the last undisputed draft as being the basis of the contract between you and the supplier.

• If a particular point is important to you, make sure that you get it in writing from the supplier. It may well be that a critical aspect is not dealt with in the supplier’s draft contract at all.

• Make sure that you get the supplier to agree to supply support and maintenance for the products purchased for a decent length of time, for example five years. You do not want the supplier cancelling support after a couple of years just when your new system is working well.

• Make sure that the procedure for acceptance testing is known and agreed.

• Make sure that you can get access to the source code of the software programs supplied if the supplier either goes into liquidation or stops supporting the software. Ideally, this source code should be deposited with an independent third party and kept updated by the supplier as each new version comes out.

• Finally, never forget that the contract is a delivery mechanism for ensuring that a project is completed in the right way at the right time by the right person and for the right price. No more, no less.
fixed price 4
force majeure 2, 25, 30
FSF (Free Software Foundation) 166, 167, 175, 193, 194
GDPR (General Data Protection Regulation, 2018) 19, 20, 65, 96
GDPR and data protection 96–115
  accountability 104
  accuracy 103
  automated processing 109–10
  consent 100–1
  data covered 96–7
  data minimisation 103
  data protection principles 98–104
  enforcement powers 112–13
  exemptions 110
  fairness 101
  fines 113–14
  individual rights 104–10
  integrity and confidentiality 104
  privacy notice 101
  purpose limitation 102–3
  remedies 111–12
  special categories 97–8
  storage limitation 103
Gh0st RAT 59
GENIVI alliance 174
Google 19, 106, 115, 153, 165, 171, 177
Google Cloud 13, 14
GPL (General Public Licence) 175, 184, 185, 187, 188, 192
hacking/hacktivism 57, 58, 59, 60–1, 64, 65, 67, 68, 69, 73, 79, 147
hardware
  licence 4
  maintenance 4
  maintenance contracts 9
  purchase 4
  purchase contracts 8–9
heads of agreement document 214
health and safety 156–61
Health and Safety at Work Act (1974) 156, 157
HPL (Honest Public Licence) 175
IaaS (Infrastructure as a Service) 13, 14, 24
IASME (Information Assurance for Small and Medium Enterprises) 77, 90
IBM 15, 172, 193, 195
ICO (Information Commissioner’s Office) 19, 58, 64, 112, 113, 119, 123–5, 131, 134–6, 137, 141
ICS (industrial control systems) 60, 62
identity theft 58, 61
IEC (International Electrotechnical Commission) 77, 89, 90
Impact Team 59
insurance 5, 51, 61, 83–4, 94, 189, 190, 207
integrators 23, 24
intellectual property law 36–50
  authorised sales 37
  copyright 36, 38, 40, 41, 42, 44, 45, 46–7
  databases 40–1, 46
  decompilation 39
  designs 49–50
  domain names 42–3
  hardware 37
  licence transfer 39
  main types of intellectual property 36
  moral rights 46
  patents 46–7
  software 38–9
  trade marks 43–5, 48
  websites 41–2
intellectual property rights 5, 32, 36–50
  authorised sales 37
  copyright 36, 38, 40, 41, 42, 44, 45, 46–7
  databases 40–1, 46
  decompilation 39
  designs 49–50
  domain names 42–3
  hardware 37
  licence transfer 39
  main types of intellectual property 36
  moral rights 46
  patents 46–7
  software 38–9
  trade marks 43–5, 48
  websites 41–2
IT in the workplace 143–55
  action plan 148
  business emails 147–8, 150
  copyright 143, 148, 154
  disclaimers 147
  DSE (Display Screen Equipment) Regulations 158–60
hacking 147
health and safety regulations 157–61
health and safety responsibilities 156–61
interception of communications 145
monitoring internet use 144–5
policies 143–7
private email 146
social media 152–3
social media policy example 153–4
staff policy 146–7
staff policy example 148–52
unauthorised websites 146
iterative methodology 197, 199, 200
joint ventures 136, 212–26
  agency agreements 218
  ‘bolt-on’ terms 218–19
  business plan 214–15
  case study 213
  competition law 223–4
  day-to-day management 215
  distribution agreement 218
  establishing 214–16, 217
  exit arrangements 216, 219
  heads of agreement document 214
  intellectual property 215
  licensing and royalties 218
  limited companies 221
  limited liability partnerships 220
  limited partnerships 220
operating agreement 222, 225–6
partnership agreement 219–20
structure 216

key personnel 5
keylogger 66
keywords 45

Law Society 2, 50, 137
Legal 500 2
letter of intent 3
level of risk 2, 69
LIA (Legitimate Interest Assessment) 122, 123
licence agreements 5, 6, 222
‘licence-in, licence-out’ policy 192
linking and framing 44–5
Linux 171, 172, 175, 183, 185, 186, 189, 191, 192–3, 194–5
litigation 231–4
LLP (Limited Liability Partnerships) 217, 220–1
maintenance contracts 6–7, 9, 38, 40
malware 57, 58, 59, 61, 62, 68, 87
Management of Health and Safety at Work Regulations (1999) 157
mediation 236–8
metatags 44, 45
MFA (multi-factor authentication) 62, 79, 82
Microsoft 15, 36, 67, 159, 165, 172, 175
Microsoft Azure 13, 14, 20
MitM (man in the middle) 67
multi-tenant 14
MVP (Minimum Viable Product) 206, 208, 209
Myanmar 60

National Cyber Security Centre 52, 84
NHS (National Health Service) 5, 51, 53
NIS (Network and Information Systems) Regulations (2018) 71, 72
NIS/Cyber Security Directive (2016) 70

NIST (National Institute of Standards and Technology) 13
cyber security framework 88–9, 93
object code 90, 91, 165, 167, 175, 185
OEM (Original Equipment Manufacturer) 218
OES (Operator of Essential Services) 70, 71
OIN (Open Invention Network) 194
Open Office 172
open source software 165–96, 216
benefits and risks 170
business models 172–3
cloud 174–5, 188
compliance 190–1
copyright 167, 169, 183, 185, 187, 191, 192, 193
definition 165–7
deployed on-premise 175, 181
developer certificate of origin 193
dual licensing models 185
employees 191–2
four freedoms 166
FSF 166
GENIVI alliance 174
in the supply chain 189–90
legal protection 167
licence compatibility 184
licences 167–9, 182–5, 186–8, 192, 194
Linux 171, 172, 175, 183, 185, 186, 189, 191, 192–3, 194–5
open source code 170–2, 174, 181, 182, 187–9, 191, 193, 194, 195
open source community 171–2
OSI 166
patents 193–4
procured on-premise 185–6
table of licences 176–80
warranties and indemnities 189
OpenChain Project 186, 189, 190, 191
operating agreement 222, 225–6
OSI (Open Source Initiative) 166, 167
OSL (Open Software Licence) 175, 184, 185
PaaS (Platform as a Service) 13, 14, 24, 69, 80
Partnership Act (1890) 220
partnership agreement 219–20
passing off 44, 45, 48
passwords 65–6, 79, 87
patents 36, 37, 46–7, 167, 193–4
payment arrangements 4, 7
PCI DSS (Payment Card Industry Data Security Standard) 77, 91
penetration tests 78, 93
permissive licence 167, 169, 173, 182, 183, 184
perpetual licence 5
Ponemon Institute 52
preventive maintenance 9
Privacy and Electronic Communications Regulations 2003 74–5, 96
ransomware 51, 53, 57, 61, 83
RDSP (Relevant Digital Service Providers) 71–2
right of access 104, 105–6, 108
right to data portability 102, 104, 108
right to erasure 104, 106–8
right to object 46, 104, 105, 109
right to rectification 104, 106
risk assessment 2, 19, 27, 30, 156, 157, 163

SaaS (Software as a Service) 13, 14, 15, 21, 24, 30
SAR (Subject Access Requests) 125–6
’scope creep’ 200, 207, 227
sequential methodology 11, 199, 200, 207, 208, 209
shadow IT 66, 67
SLA (service level agreement) 10–11
social media 13, 80, 82, 93, 127, 152–4, 165, 171
Society for Computers and Law 2
software
application software 4
development contracts 7–8
intellectual property rights 38–40
licence agreements 5, 6
licences 5, 6, 38, 39, 169
maintenance 6
operating system 4
security 84
source code 8, 12, 39, 90, 91, 165–7, 169, 181, 183, 185, 187, 188
SSD (solid-state drive) 14
staff policy 146–52
Study on Global Megatrends in Cybersecurity 52
subscription agreement 14
termination 5, 7
‘The cathedral and the bazaar’ 171
time and materials 3, 4, 8, 201, 205, 206, 207
Torvalds, Linus 171
trade marks 36, 41, 42, 43–5, 48, 49, 194, 216
UK design right 50
vulnerability assessments 78, 93
WannaCry and Petya attacks 53
‘waterfall’ development 11, 171, 199, 209
WhatsApp 13
WikiLeaks 59
Workplace Regulations (1992) 157
World Intellectual Property Organization 43
A PRACTICAL GUIDE TO IT LAW
3rd edition
Edited by Jeremy Holt and Jeremy Newton

IT-related legal issues are faced by businesses on a daily basis, however, the legal concepts and terminology involved are often notoriously difficult for non-specialists to grasp.

This comprehensive guide explains the practicalities of IT law in plain English, including relevant legal frameworks and accompanying technical context, and is ideal for management professionals working in IT Law, or those studying for entry to the field.

The book examines and discusses key topics, including examples and tips, providing you with the tools you need to work out what needs to be done, who to get advice from and how to deal with IT and legal experts.

- Written by a diverse group of IT law professionals
- Suitable for IT and management professionals with no prior knowledge of IT law
- Covers IT contracts, IT in the workplace, intellectual property law, legalities around setting up joint ventures, resolving disputes, open source software
- Includes brand new chapters on GDPR, cyber security, cloud computing contracts and Agile projects

ABOUT THE AUTHORS
Jeremy Holt is the former head of the Computer Law Group of Clark Holt Commercial Solicitors. Jeremy Newton is a director at Technology Law Alliance in London, a law firm specialising in IT, outsourcing and e-commerce law.

You might also be interested in:

A tour de force in taking readers through complex IT law issues in clear, easy to understand fashion. From IT contracts to IP and data protection law, this book is bang up to date with the latest changes in one of the most fast moving fields.

Susan Singleton, IT Lawyer, Singletons Solicitors

An engaging book, equally accessible to those from an IT, legal or business background... brings to life by application what might sometimes be dry areas. I learnt from it, and the learning was enjoyable.

Prof. Angela Devereux, Director of Professional Practice, Hillary Rodham School of Law at Swansea University

The Swiss Army knife of IT Law, this is like having 13 separate essential guides in one book, each independent but linked to the core topic of IT Law and how to interpret and navigate it, giving you common sense advice and approaches for everyday use.

Peregrine R Perrott, Global Head of Commercial, Compliance and Regulatory, Faria Education Group

Information Technology, Law, Business

Cover photo: ©Stock © Lebazle

ISBN 978-1-78017-488-4

Paperback available