6b

Your business @ risk: Information security awareness

Shropshire and Wrekin Fire Authority

Audit 2009/10

audit commission

The Audit Commission is an independent watchdog, driving economy, efficiency and effectiveness in local public services to deliver better outcomes for everyone.

Our work across local government, health, housing, community safety and fire and rescue services means that we have a unique perspective. We promote value for money for taxpayers, auditing the £200 billion spent by 11,000 local public bodies.

As a force for improvement, we work in partnership to assess local public services and make practical recommendations for promoting a better quality of life for local people.

Contents

Background **2**

Main conclusions **3**

Main findings **4**

Perceptions of the Authority's IT security arrangements (Figures 1-2) 4

Staff awareness of IT security policy and associated legislation (Figures 3-4) 5

Password security (Figures 5-12) 7

Maintaining an audit trail (Figure 13) 12

Accessing inappropriate material on the Internet (Figures 14-16) 13

Sharing personal data (Figures 17-19) 15

Access to confidential data when out of the office 17

Using untrusted media 18

Recovering lost data 21

Appendix 1 Survey responses **22**

Background

1 The growth of the e-agenda, the increase in the use of new technologies, greater public access and more joined-up working are all positive trends but all mean increased risks for public sector bodies. Computer viruses, IT fraud, hacking, invasion of privacy and downloading of unsuitable material from the Web all remain real threats. Recent media coverage has given information security risks a high profile by highlighting losses of personal information by a range of government bodies.

2 Where the above risks have materialised, they have usually been attributed to failures in governance. Organisations must therefore address information governance issues if the increased use of new technology is not to be matched by a decrease in public confidence in the security of the information held by public bodies.

3 In response, the Audit Commission has updated its information governance tool, 'Your Business at Risk' (YB@R). The updated survey tool provides an assessment of compliance with information governance procedures and helps authorities to reduce the risk of information security breaches. It should be noted, however, that the tool is not designed to measure the extent to which bodies are meeting specific government guidelines on data handling, and it should not be taken to do so.

4 As part of our 2009/10 audit at Shropshire and Wrekin Fire Authority (SWFA), 100 staff were selected by the Authority to be representative of the wider staff base. These selected given access to the YB@R survey on the Audit Commission's secure extranet website. All staff were asked to complete the survey during the period April/May 2010. We received 65 responses, a return rate of 65 per cent. This is a good response rate and is representative of the general staff population.

Main conclusions

5 The overall perception of most staff is that IT security at the Authority is adequate or better and that all staff have a role to play in it.

6 Regular reminders to staff about all of the issues covered in our survey will be of benefit to the Authority. However, our survey indicates that there are key areas where the Authority particularly needs to raise staff awareness. These are:

- using appropriately secure mechanisms to share personal data outside the Authority (paragraph 19). Over half would use unsecured e-mail, and 20 per cent would use standard post.
- using a secure method of accessing Authority data when working out of the office (paragraph 20). Over three quarters of respondents use relatively insecure methods of accessing confidential Authority data from outside the office/work environment.
- consideration of data risk from accessing untrusted/unknown sources (paragraph21). About one in five would put an unknown CD or memory stick straight into a works computer.
- the Authority's rules on the use of its IT resources (paragraph 10), with (30 per cent) not being entirely clear on the Authority's rules on the use of its IT resources
- The need for security of passwords (paragraph 11), with half writing passwords down, and of those that do write them down, 70 per cent store them insecurely on personal paper documents, such as diaries.
- keeping log-on details secure, for example, not revealing them over the phone or Web (paragraphs 14 and 16). 20 per cent would give a password over the phone when they did not instigate the contact.
- reporting information security incidents (paragraph 15).
- the importance of back up procedures (paragraph 22).

7 The detailed findings on which our conclusions are based are shown in the following section.

Main findings

8 We asked staff twenty-five information security questions. A summary of the responses on which our findings are based is attached at Appendix 1. The main findings at SWFA are set out below. We have shown, in graph format, the question and responses that form the basis for each of our findings.

Perceptions of the Authority's IT security arrangements (Figures 1-2)

9 Most respondents had a positive view of the Authority's IT security arrangements (Figure1), but were slightly less confident that other organisations surveyed. The were mostly clear that all Authority staff have a part to play in it (Figure 2)

Figure 1: **IT security - How would you describe your organisation's IT security?**

93.8 per cent of respondents rated the Authority's IT security adequate or better.

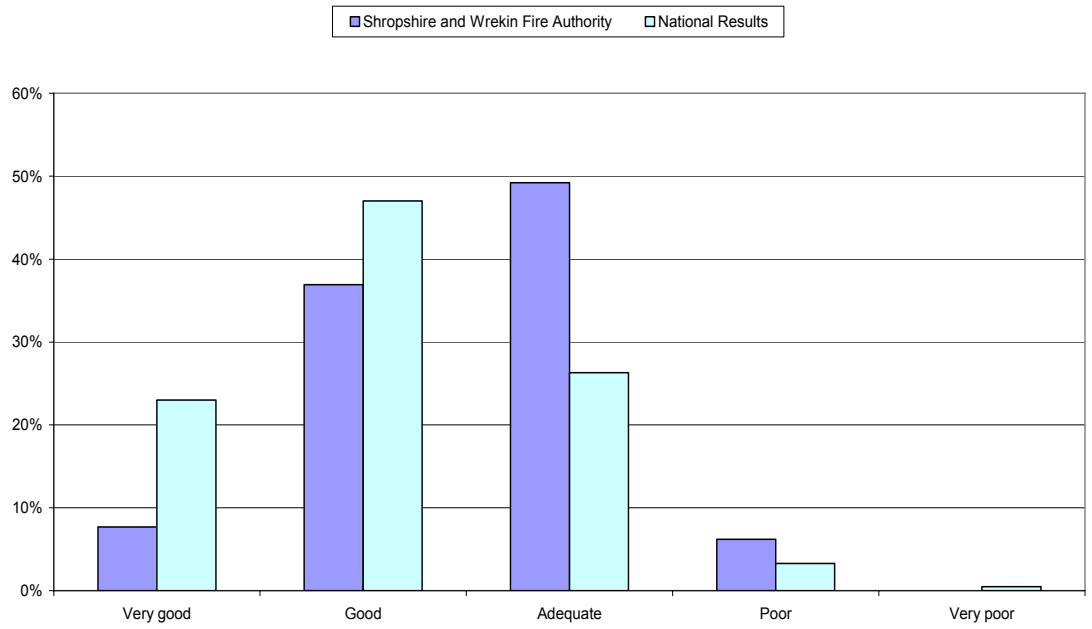
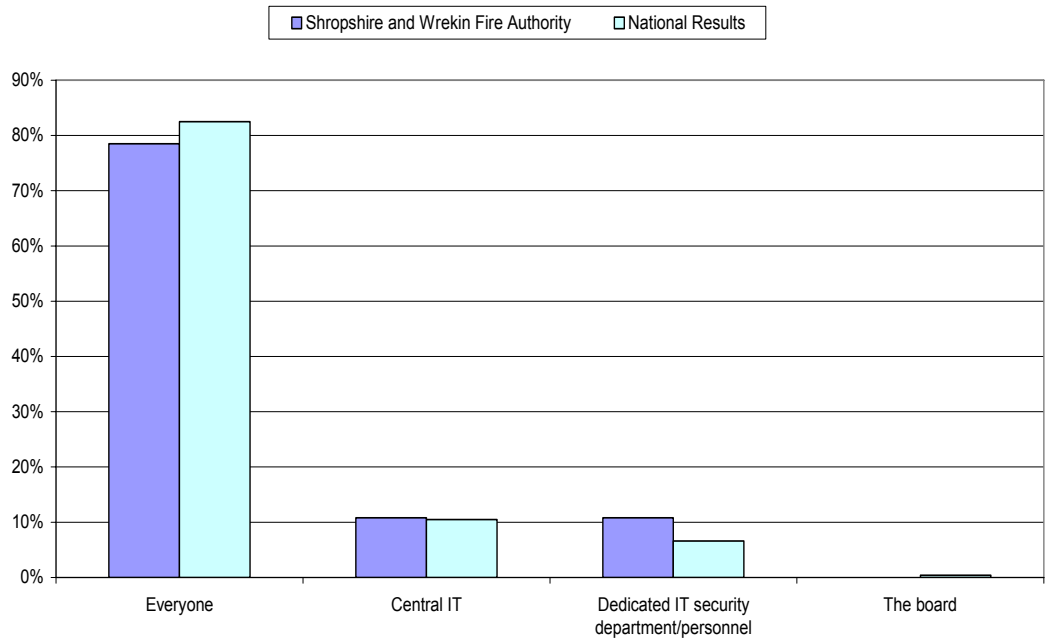


Figure 2: **IT security responsibilities - Who is responsible for IT security in your organisation?**

78 per cent of respondents were clear that all staff have a role to play in IT security



Staff awareness of IT security policy and associated legislation (Figures 3-4)

10 A necessary foundation for effective IT security is that staff are clear about the Authority's policies and the associated legislation. Most respondents' understanding of the legislation on protection of personal data is good (Figure 3). However, many respondents (30 per cent) are not entirely clear on the Authority's rules on the use of its IT resources (Figure 4).

Figure 3: **Awareness of Data Protection law - Which of the following are covered by the Data Protection Act if your organisation holds information about a living individual?**

More than 84 per cent of respondents were aware of the full range of media covered by Data Protection law.

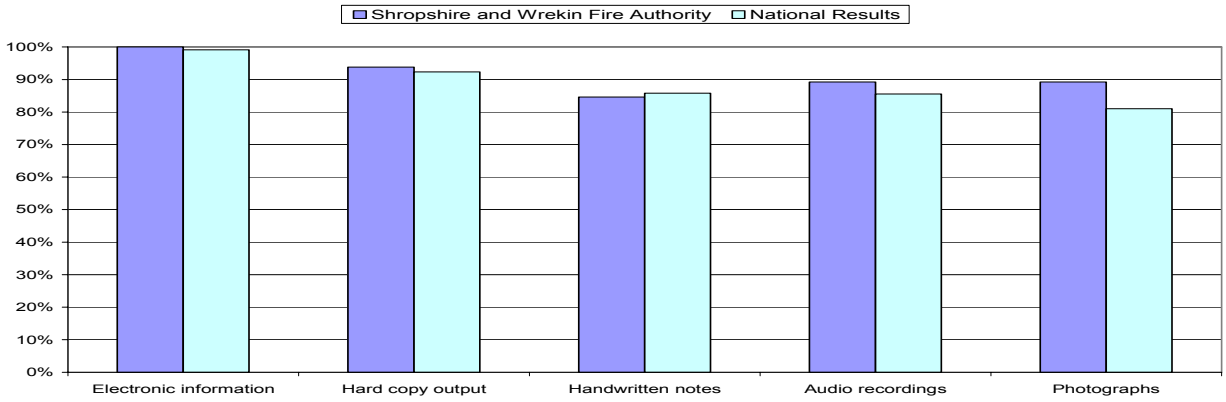
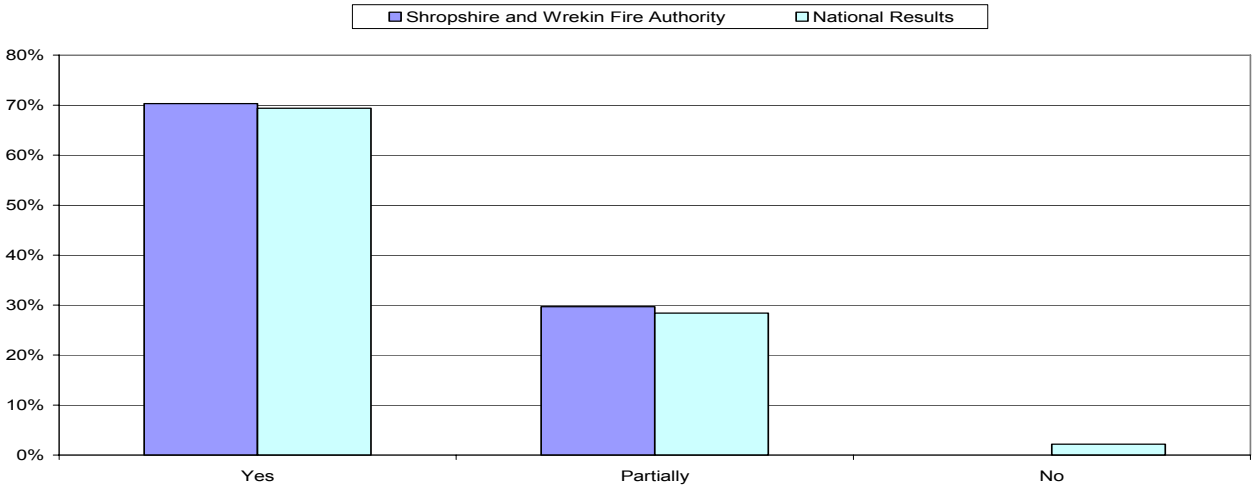


Figure 4: **Awareness of the Authority's rules about use of IT resources - Are you aware of your organisations rules about the use of IT resources such as: internet, email and telephones?**

Only 70 per cent of respondents were confident they knew all the Authority's rules on use of IT resources



Password security (Figures 5-12)

11 Most public sector bodies use passwords as the main method of authenticating access to information systems. Best practice is that the strength of the access control is based on the sensitivity of the information and the degree of access being given. In practice, this often means that many staff have to remember a number of complex passwords and in order to do so may need to keep a record of them. We found that to be the case at SWFA and we found scope for raising awareness of how to reduce the associated risks (Figures 5-7).

Figure 5: **Writing down passwords - Do you feel it is necessary to write some or all of your passwords down?**

Over half of respondents keep a written record of their passwords

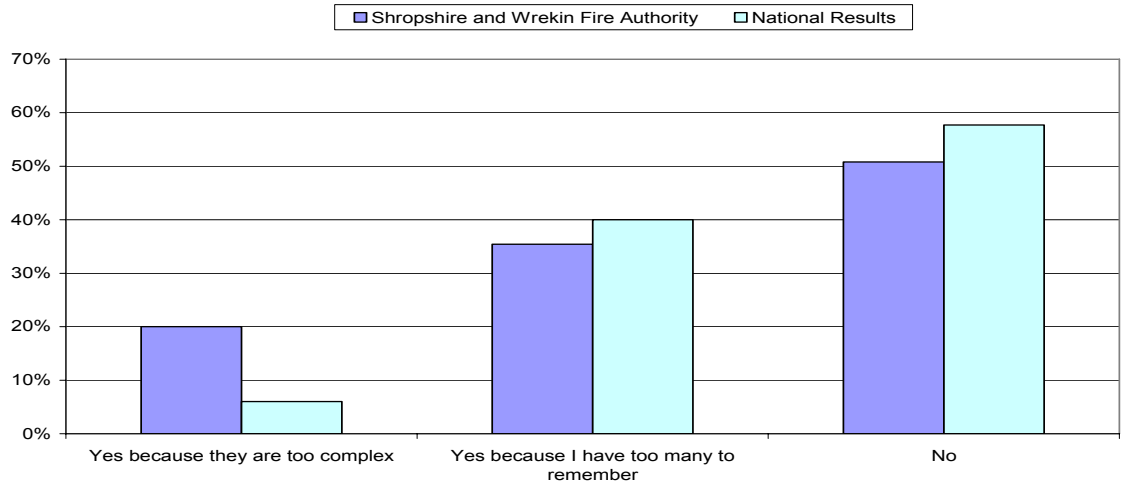


Figure 6: **Storing records of passwords - If yes, how do you store them?**

Just 70 per cent of respondents are storing a record of their password insecurely

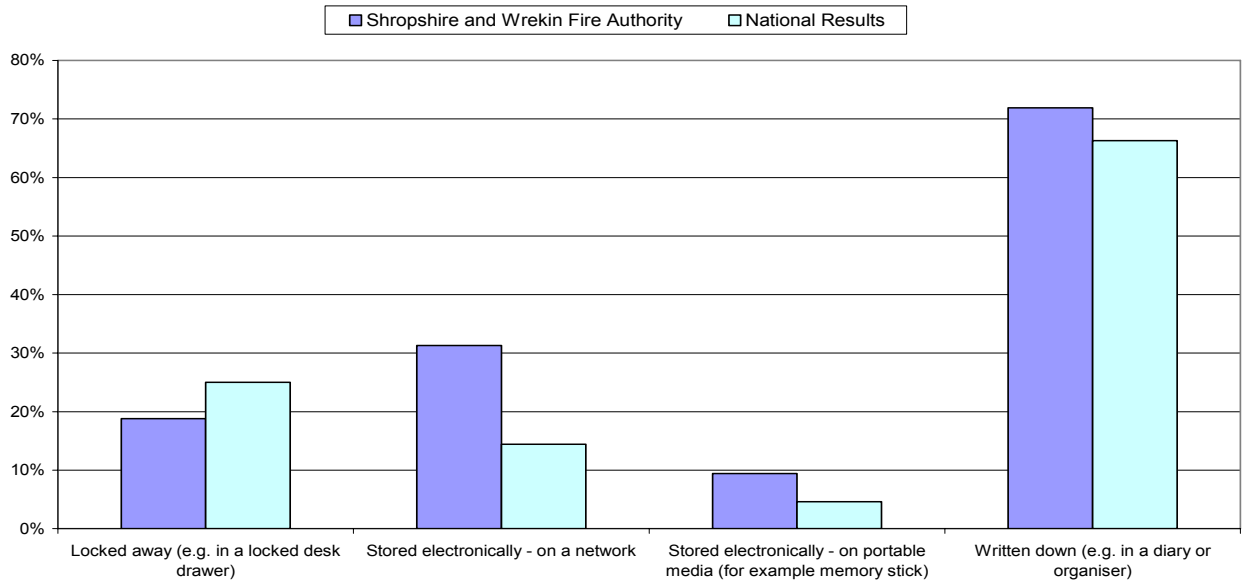
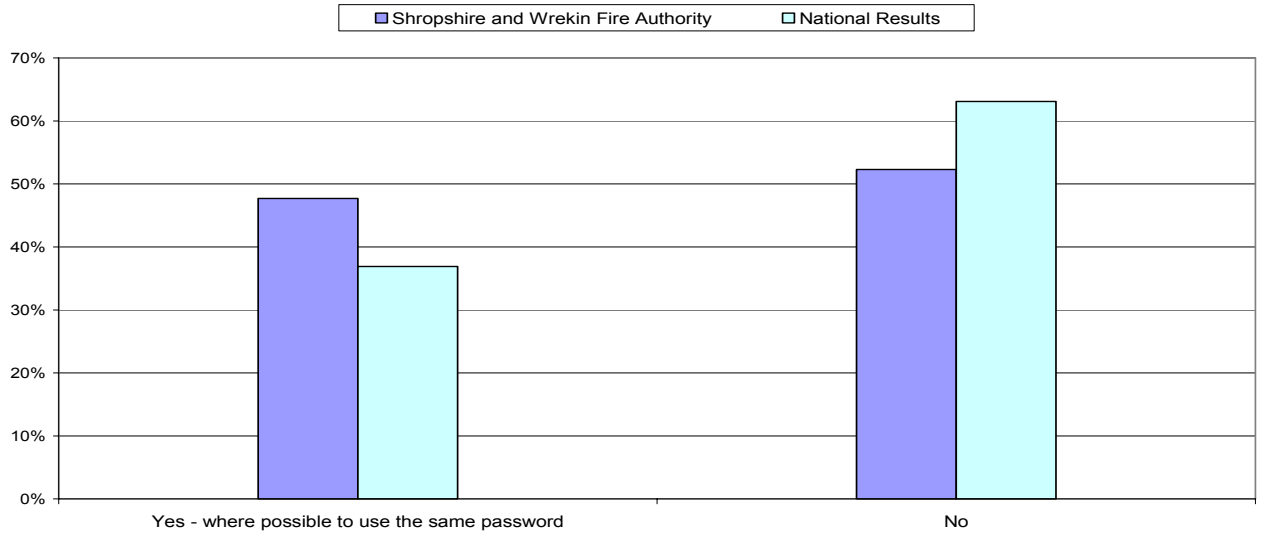


Figure 7: **Use of same password across systems - Do you use the same password across all systems you need to access**

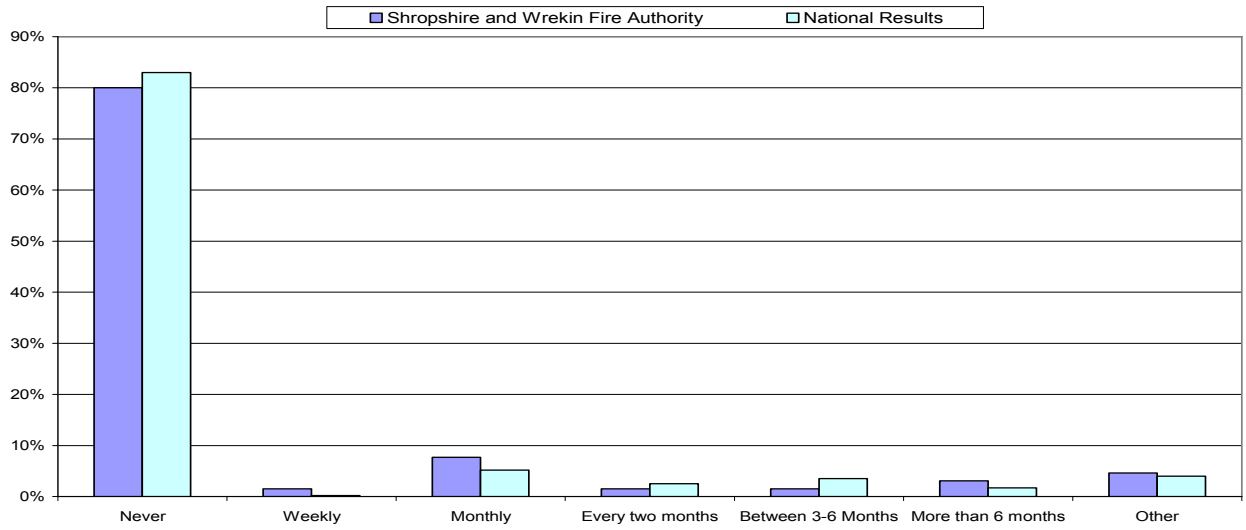
About a third of respondents use the same password across all their systems.



12 Passwords should be changed periodically, at a frequency based on the criticality of the information. Best practice is to enforce a change and notify the user before the expiration date. Most respondents reported that they rely on automatically enforced password changes (Figure 8)

Figure 8: **Changing passwords - How often do you voluntarily change your passwords**

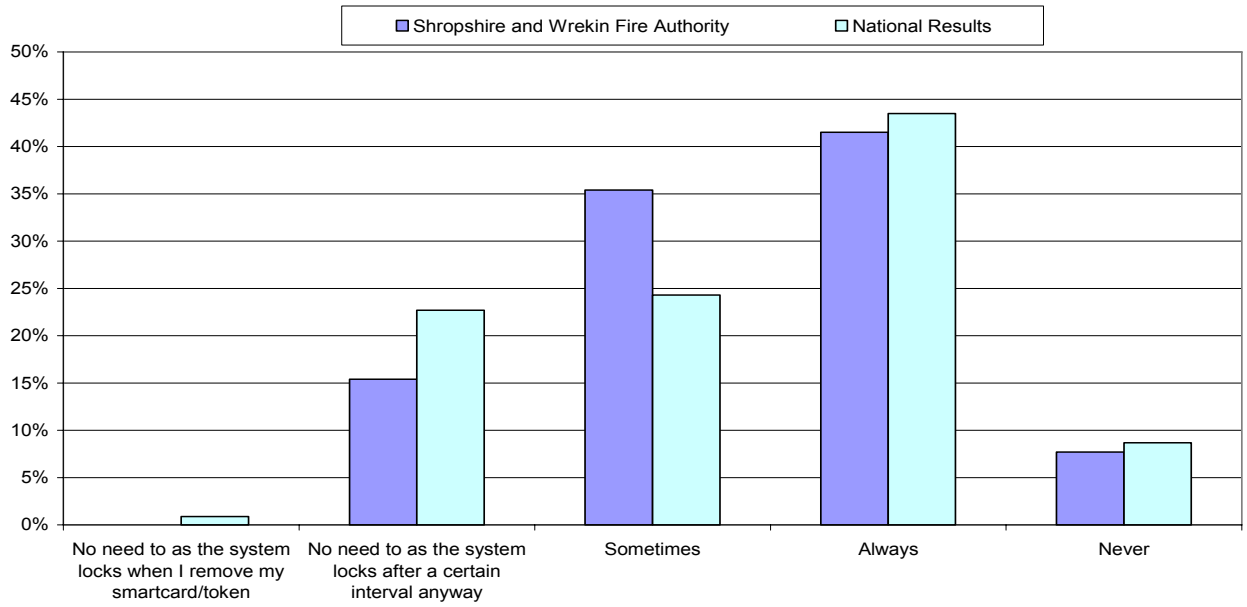
Most respondents rely on the system to force a password change. In a small minority passwords are being changed less frequently than monthly



13 Part of an effective access control process is a process to disconnect a log-on session if no activity has occurred for a period of time. The most secure approach is for the system to automatically do so after a period of inactivity, which was reported as happening at SWFA for a small percentage of respondents. However, over 90 per cent do not lock their PC (using Ctrl/Alt/|Del) if they leave it unattended.(Figure 9)

Figure 9: **Locking down the PC - Do you lock (for example CTRL+ALT+DEL) your computer when leaving it unattended**

Just over half of respondents leave their computer unlocked and unattended on occasions



14 The human factor is widely considered to be the weakest link in the information security chain. Authorities with strong technical security measures may still fail to protect their information systems if a member of staff gives away confidential information such as passwords, for example over the phone, by email or via the web. The best means of defence against this is to raise staff awareness of the risk. We found scope for raising awareness of these so called 'social engineering' risks at SWFA (Figures 10-11).

Figure 10: **Revealing log-on security details over the phone - You receive a call from an IT help desk operator about a problem you've been having with your PC, what information would you give them if asked?**

Almost half of respondents would reveal their log on id to a caller, and 20 per cent would reveal their password.

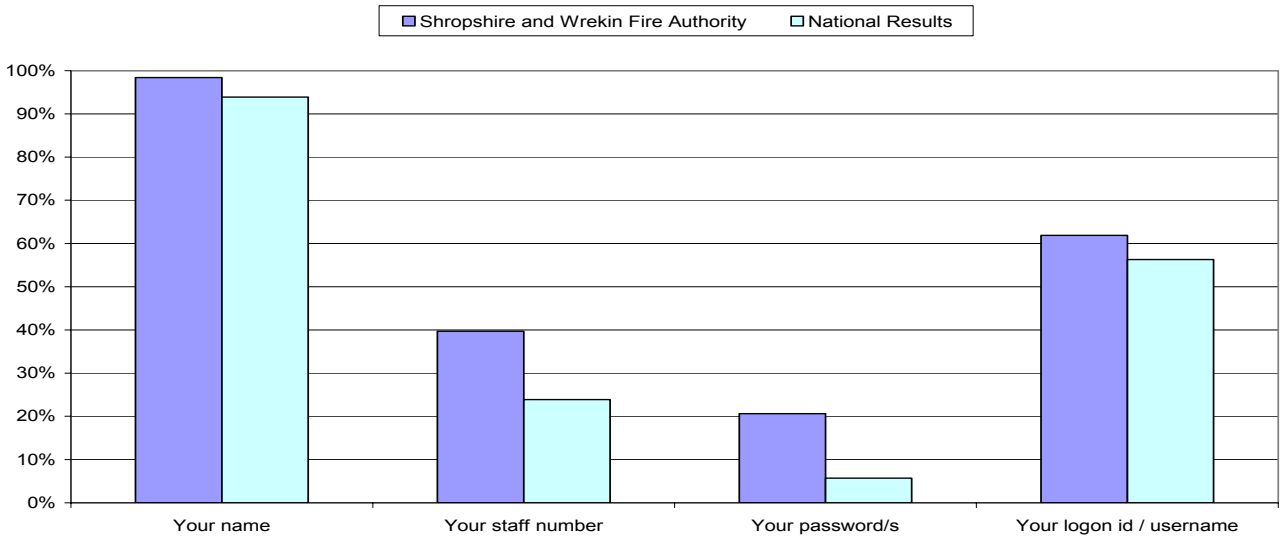
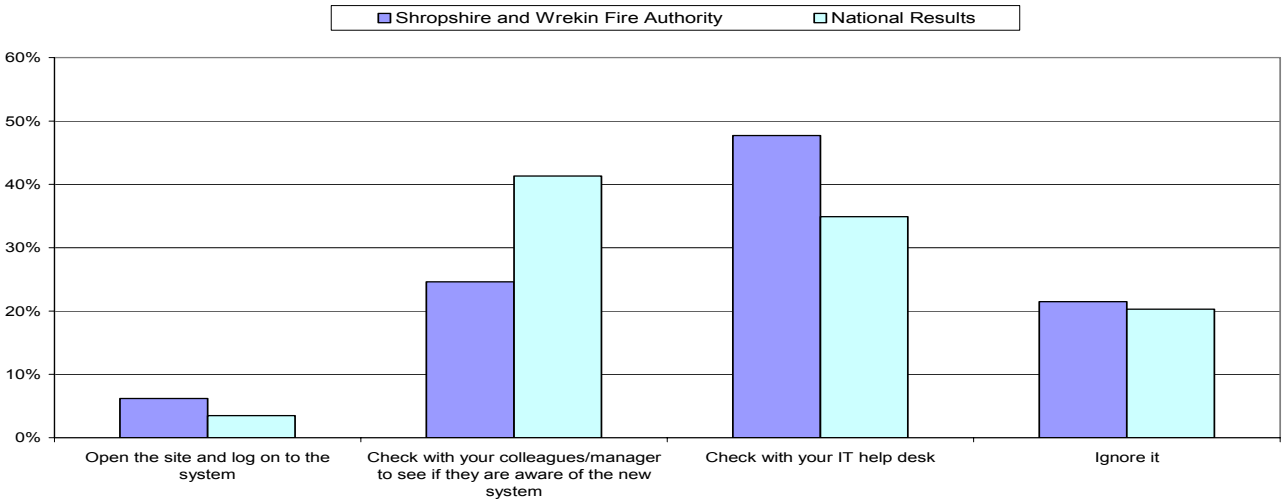


Figure 11: **Revealing log-on security details over the web - You receive an e-mail telling you of a new corporate system and asks you to open a web page and log on using your network user name and password. This is the first you have heard of this system - what would you do next?**

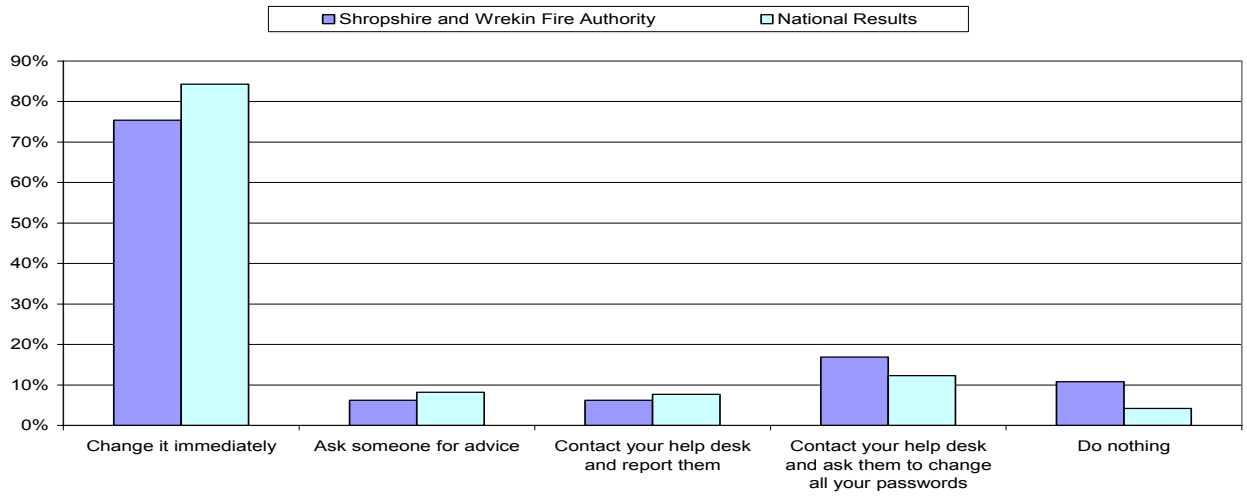
Nearly a quarter of respondents would not report an unexpected web request for them to reveal their log-on details. A minority (about 6.2 per cent) would submit their details, which is almost twice the level observed at other organisations surveyed.



15 Part of recognised good practice in information security is managing security incidents; including making staff aware of the procedures for reporting different types of incident. Figure 11 and Figure 12 (shown below) indicate that there is scope for raising staff awareness about reporting information security incidents

Figure 12:**Response to a revealed password - What would you do if you suspect that someone knows your password**

More than 75 per cent of respondents would change their password if it had been revealed, but only 6 per cent would report it as a potential security incident

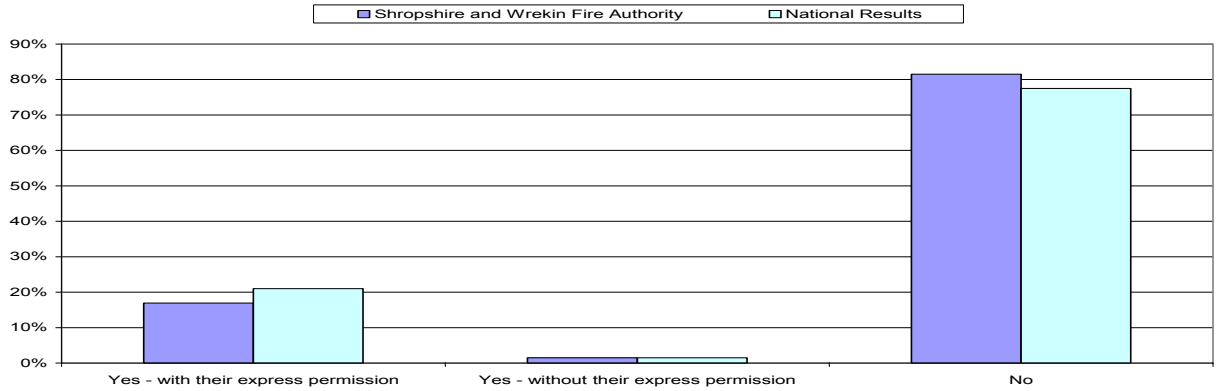


Maintaining an audit trail (Figure 13)

16 Sharing log-on accounts and passwords, even with permission, reduces the ability to audit malicious activity, conflicts with accepted good practice and infringes data protection principles. At SWFA, a significant minority of respondents had recently used someone else's log-in, without their permission.

Figure 13:**Using a colleague's log-in - In the last three months, have you ever used or accessed a computer that has been logged in under someone else's password**

About a quarter of respondents had recently used a computer logged in under someone else's identity.



Accessing inappropriate material on the Internet (Figures 14-16)

17 Any use of Authority computers to access inappropriate (for example, illegal or sexually explicit) material on the Internet exposes the Authority to the risk of reputational damage. There was a low incident at your Authority, but still significantly higher than the average. Just over 10 per cent had recently seen colleagues viewing material that would damage the Authority's reputation (see Figures 14-15).There is scope for the Authority to assess its control measures, and remind staff of the rules and sanctions

Figure 14:**Viewing inappropriate material on the Web - incidence**

Over 1 in 10 of the respondents has recently seen colleagues viewing inappropriate Internet material at work. This is much higher than others surveyed

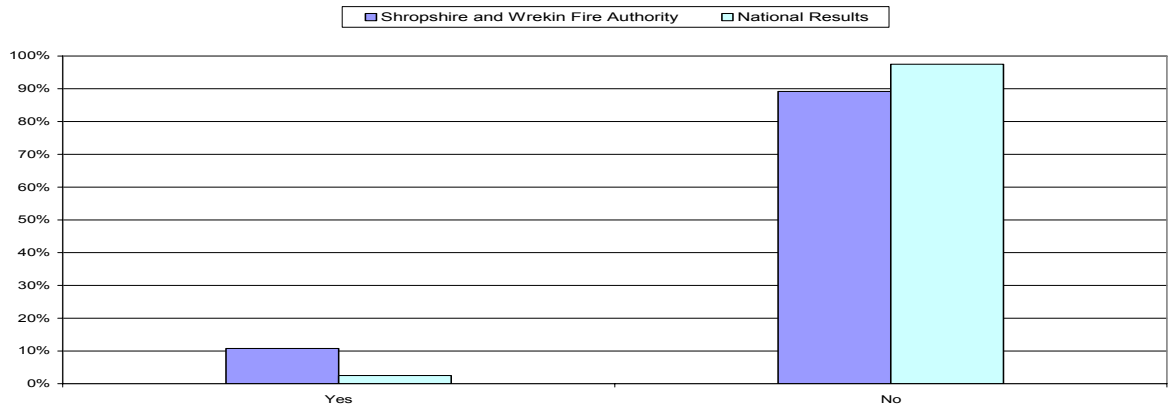
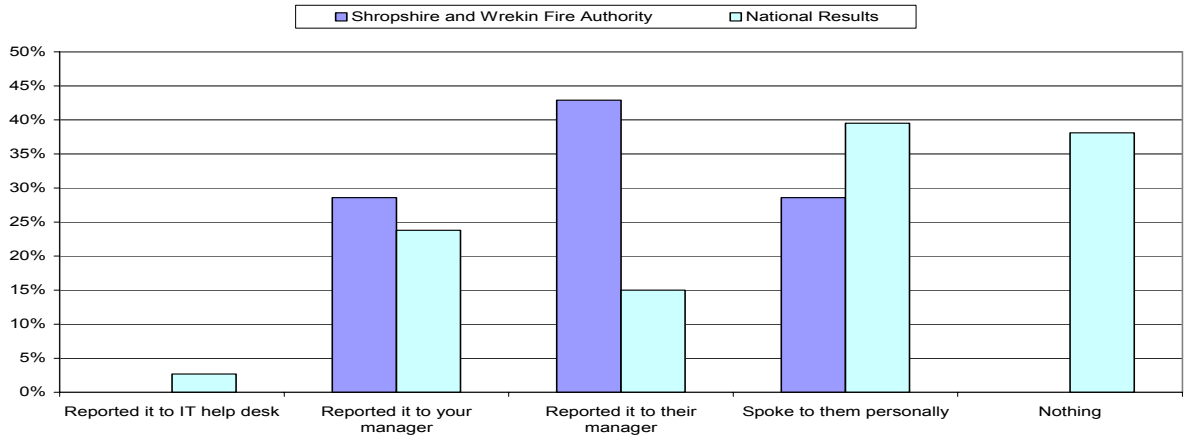


Figure 15:**Viewing inappropriate material on the Web - action taken**

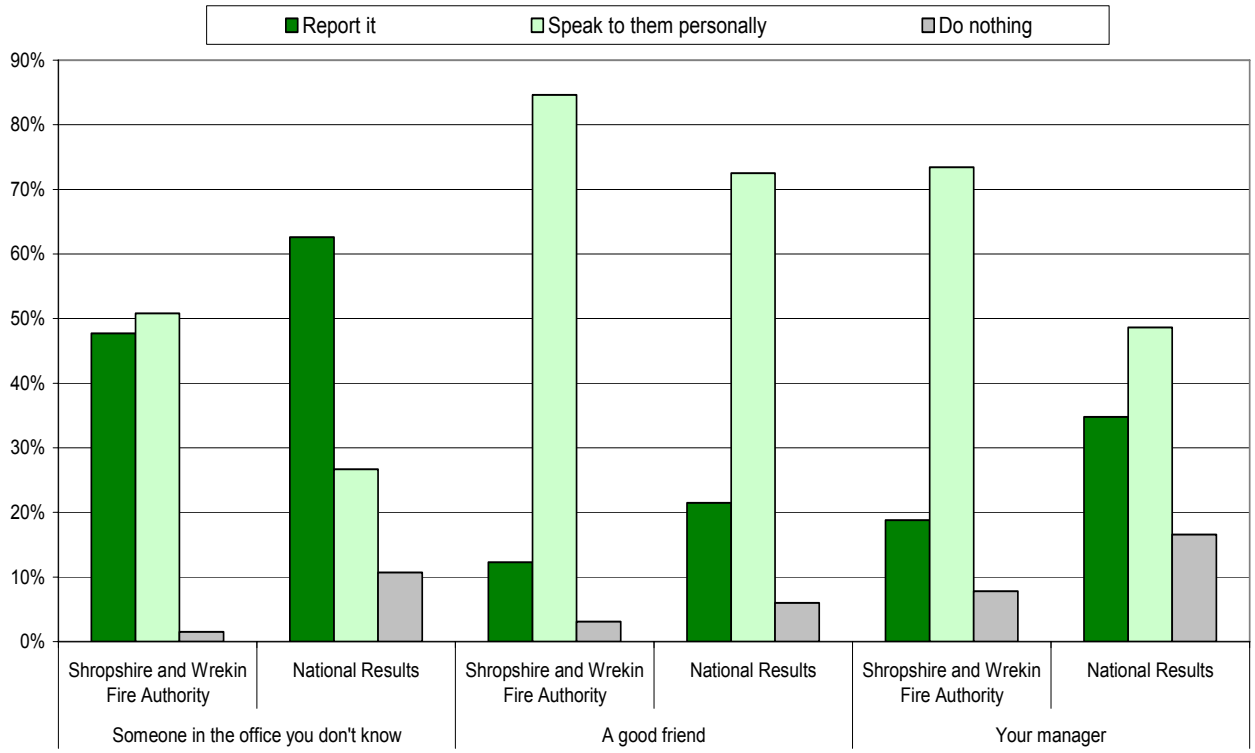
All respondents who had seen inappropriate material being accessed took some action, but it was not always raised with line managers



18 Respondents would be least likely to take action if they saw their manager accessing inappropriate material. This may indicate a need to raise awareness of or confidence in the Authority's whistleblowing procedures (see Figure 16).

Figure 16: **Viewing inappropriate material on the Web - In the future, if you saw one of the following individuals accessing inappropriate material on their work computer, what would you do**

8 per cent of respondents would do nothing if they saw their manager accessing inappropriate material



Sharing personal data (Figures 17-19)

19 With recent heavily reported events surrounding loss of personal data, loss of any data containing personally identifiable information would seriously compromise the Authority's reputation. A relatively high proportion of respondents reported that personal data is currently shared using insecure methods (Figure 17). Most respondents report that no greater security is applied when data is shared with an external party even though most considered that the consequences of incorrect disclosure would be significant (Figures 18-19). The Authority needs to ensure that the measures being applied are proportional to the sensitivity and volume of personal data being shared.

Figure 17: **Sharing personal data - If your job requires you to share personally identifiable information, how is this shared?**

Nearly 55 per cent of respondents share personal data by standard email. About 20 per cent send personal data by standard post

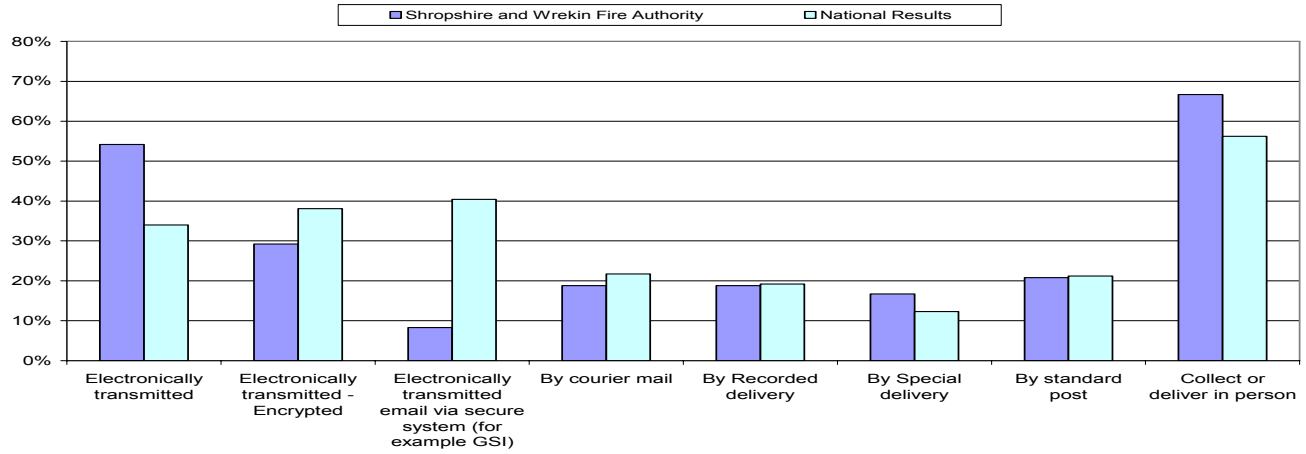


Figure 18: **Sharing personal data - Is shared information given a higher level of security if it is sent externally as opposed to internally?**

Just over 40 per cent of respondents use a more secure approach when data is shared externally.

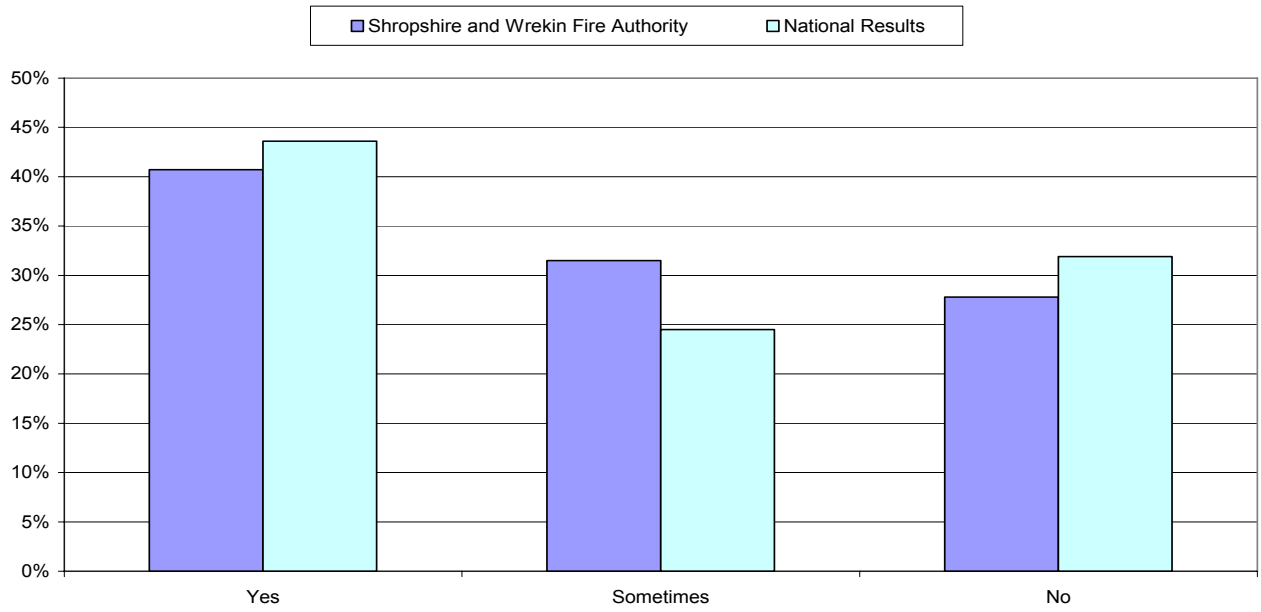
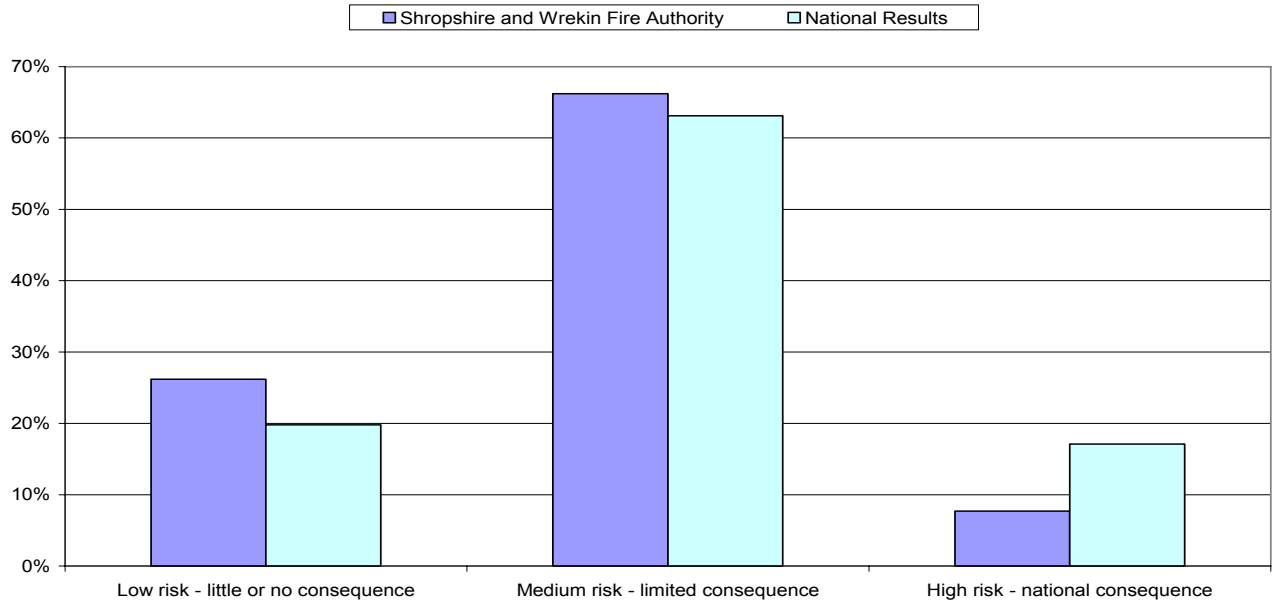


Figure 19:**Personal data - consequences of incorrect disclosure**

Nearly three quarters of respondents consider that incorrect disclosure of the personal information they routinely use would be of significant consequence (Medium to High consequence).

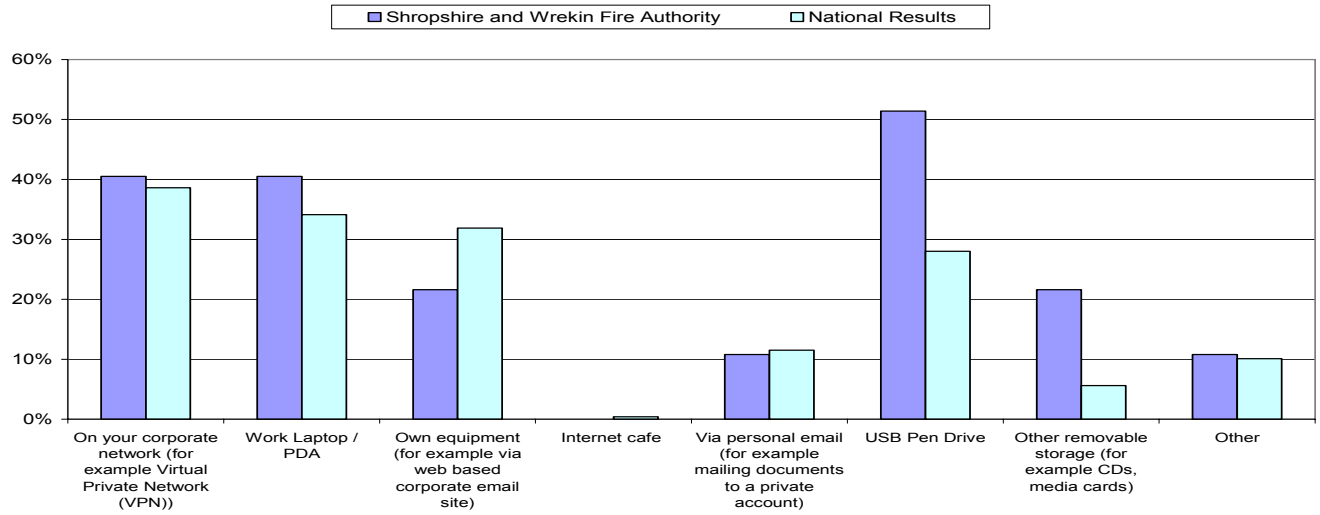


Access to confidential data when out of the office

20 The risks of unauthorised access to confidential data are increased once the data has left the IT environment controlled by the Authority (ie the Authority's network and Authority-configured PCs). Over three quarters of respondents use relatively insecure methods of accessing confidential Authority data from outside the office.

Figure 20: **Accessing confidential Authority data from outside the office - If you access work related confidential information when out of the office, how is the information accessed**

95 per cent of respondents use relatively insecure methods of accessing confidential Authority data when out of the office (ie the four categories to the right of the graph). This is weaker than the average observed.



Using untrusted media

21 Using media from an unknown or untrusted source poses a risk of introducing viruses or other malware into the Authority's network. About one in five respondents would put an untrusted CD from an external source into their work computer (Figure 20). About one in six respondents would put an unknown CD or memory stick into their computer if it had the Authority's logo on it (Figures 22-23). There is scope for the Authority to raise awareness of the risks of untrusted media.

Figure 21:**Response to an unexpected CD - You receive a free promotional CD at your work address**

Over 22 per cent of respondents would put an untrusted CD from an external source into their work computer

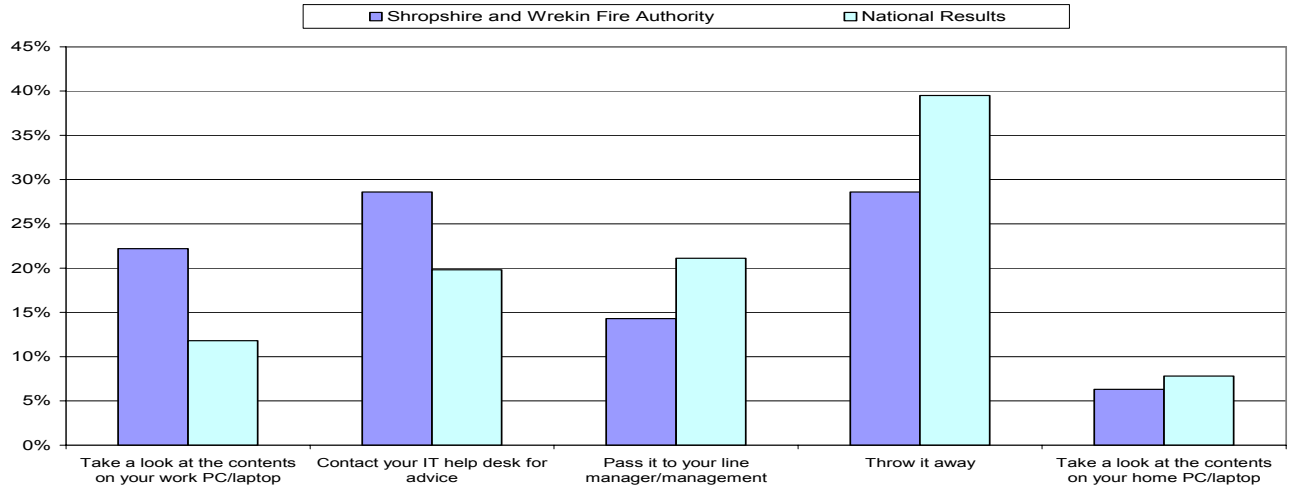


Figure 22:**Response to a CD appearing to originate from the Authority - What would you do first if you found a CD on your work desk, and it was labelled:**

Over 30 per cent of respondents would put an unknown CD into their work computer if it appeared to be an Authority CD. Far fewer would do so if it appeared to be confidential information

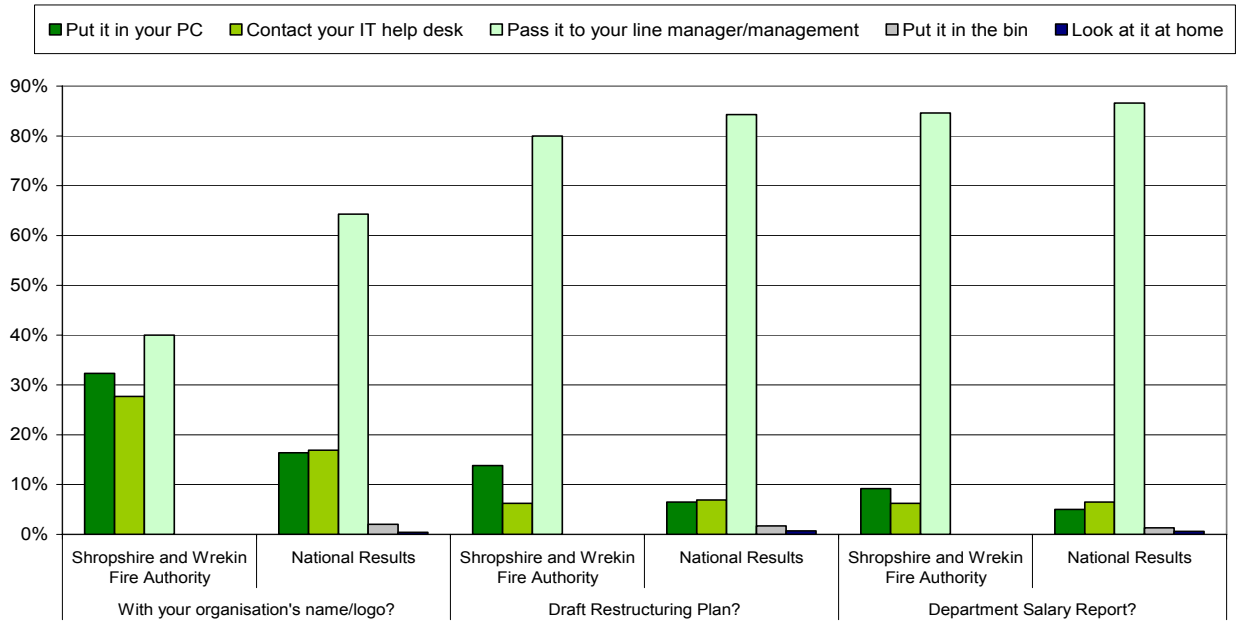


Figure 23:**Response to finding a memory stick - You find a memory stick (USB flash/pen drive) - What would you do first**

Only 3 per cent would read an untrusted memory stick on their work PC to check the contents

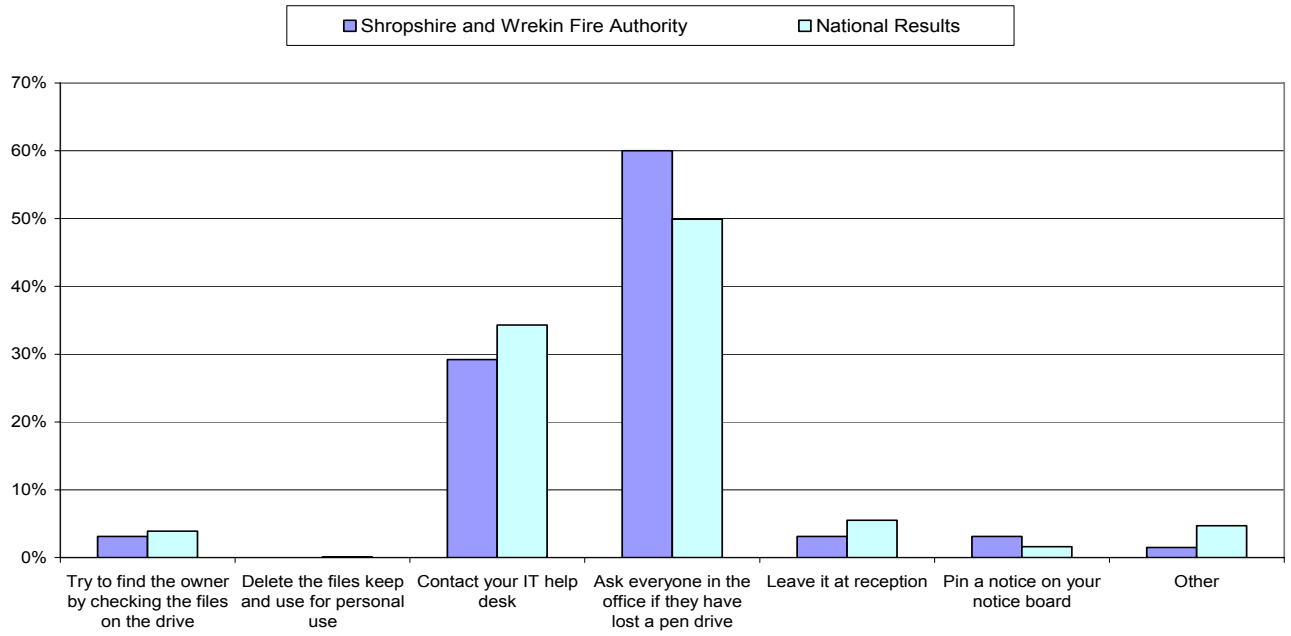
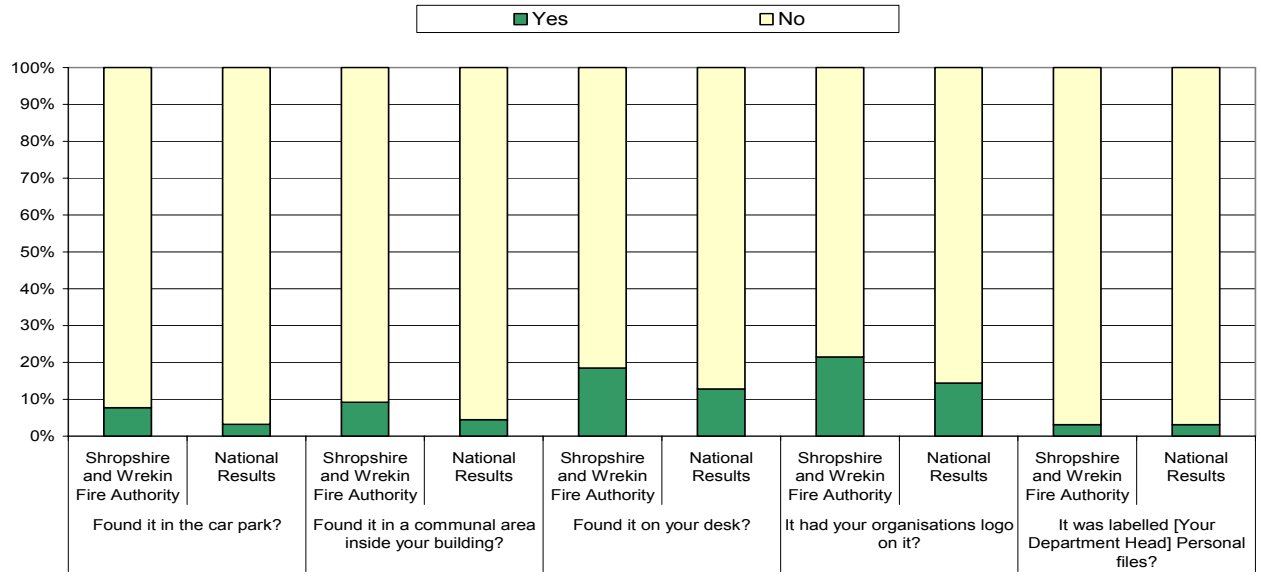


Figure 24:**Response to finding a memory stick - If you found a memory stick, would you place it in your computer if you…**

Just under 8 per cent of respondents would put into their work PC if found in a car park, and over 21 per cent would use an untrusted memory stick if it had the Authority's logo on it.

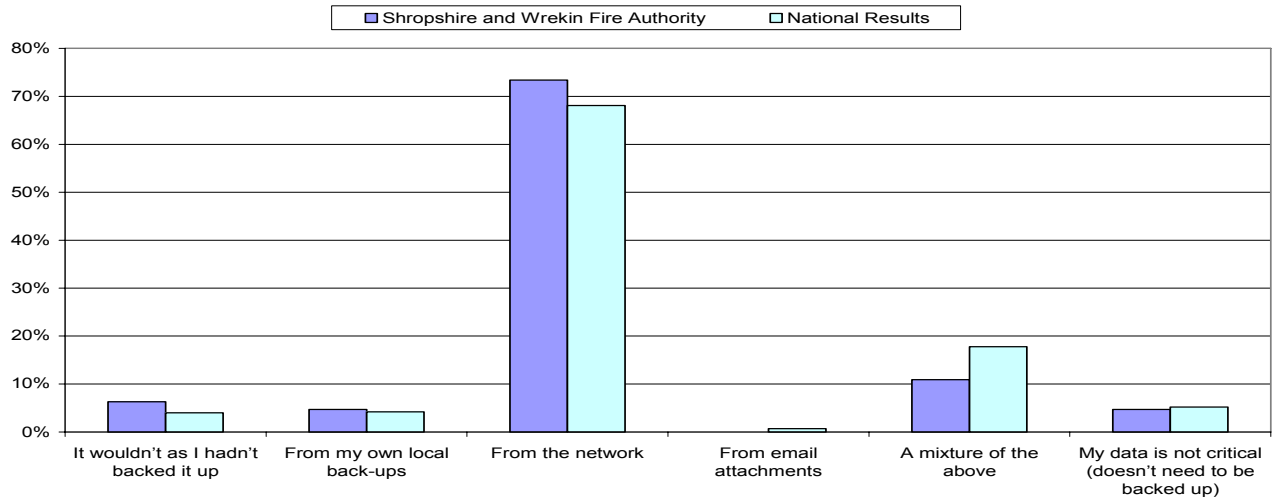


Recovering lost data

22 When computers are lost or destroyed, the consequences of losing the data on them is often more serious than the financial loss of computer equipment. Over 87 per cent of respondents were confident that their data could be recovered, mostly from back-ups to network drives. However, about 10 per cent responded that their data was not backed up, with 3 per cent who considered their data not to be critical.

Figure 25:**Recovering lost data - Your computer is destroyed and you are sent a replacement - how would your data be restored**

6.3 per cent of respondents have no back up arrangements for data that may be critical, which is higher than the average



Appendix 1 Survey responses

SWFA compared against the national responses % as at May 2010

Q1.	Do you feel it is necessary to write some or all of your passwords down? (please tick all that apply)	
	Yes because they are too complex	13 (20.0%)
	Yes because I have too many to remember	23 (35.4%)
	No	33 (50.8%)

Q2.	If yes, how do you store them? (tick all that apply)	
	Locked away (eg in a locked desk drawer)	6 (18.8%)
	Stored electronically - on a network	10 (31.3%)
	Stored electronically - on portable media (for example memory stick)	3 (9.4%)
	Written down (eg in a diary or organiser)	23 (71.9%)

Q3.	What would you do if you suspect that someone knows your password (for example someone watched you type your password in)? (please tick all that apply)	
	Change it immediately	49 (75.4%)
	Ask someone for advice	4 (6.2%)
	Contact your help desk and report them	4 (6.2%)
	Contact your help desk and ask them to change all your passwords	11 (16.9%)
	Do nothing	7 (10.8%)

Q4.	How often do you voluntarily change your passwords (that is before the system prompts you)?	
	Never	52 (80.0%)
	Weekly	1 (1.5%)
	Monthly	5 (7.7%)
	Every two months	1 (1.5%)
	Between 3-6 Months	1 (1.5%)
	More than 6 months	2 (3.1%)
	Other	3 (4.6%)

Q5.	Do you use the same password across all systems you need to access?	
	Yes - where possible to use the same password	31 (47.7%)
	No	34 (52.3%)

Q6.	In the last three months, have you ever used or accessed a computer that has been logged in under someone else's password	
	Yes - with their express permission	11 (16.9%)
	Yes - without their express permission	1 (1.5%)
	No	53 (81.5%)

Q7.	Do you lock (for example CTRL+ALT+DEL) your computer when leaving it unattended?	
	No need to as the system locks when I remove my smartcard/token	0 (0.0%)
	No need to as the system locks after a certain interval anyway	10 (15.4%)
	Sometimes	23 (35.4%)
	Always	27 (41.5%)
	Never	5 (7.7%)

Q8.	You receive a call from an IT help desk operator about a problem you've been having with your PC, what information would you give them if asked? (please tick all that apply)	
	Your name	62 (98.4%)
	Your staff number	25 (39.7%)
	Your password/s	13 (20.6%)
	Your logon id / username	39 (61.9%)

Q9.	You receive an e-mail telling you of a new corporate system and asks you to open a web page and log on using your network user name and password. This is the first you have heard of this system - what would you do next?	
	Open the site and log on to the system	4 (6.2%)
	Check with your colleagues/manager to see if they are aware of the new system	16 (24.6%)
	Check with your IT help desk	31 (47.7%)
	Ignore it	14 (21.5%)

Q10.	In the last 12 months have you seen someone viewing material on their work computer that would bring the professional reputation of your organisation into disrepute?	
	Yes	7 (10.8%)
	No	58 (89.2%)

Q11.	If you answered Yes to the previous question, what did you do? (Please tick all that apply)	
	Reported it to IT help desk	0 (0.0%)
	Reported it to your manager	2 (28.6%)
	Reported it to their manager	3 (42.9%)
	Spoke to them personally	2 (28.6%)
	Nothing	0 (0.0%)

Q12.	In the future, if you saw one of the following individuals accessing inappropriate material on their work computer, what would you do...			
		Report it	Speak to them personally	Do nothing
	Someone in the office you don't know	31 (47.7%)	33 (50.8%)	1 (1.5%)
	A good friend	8 (12.3%)	55 (84.6%)	2 (3.1%)
	Your manager	12 (18.8%)	47 (73.4%)	5 (7.8%)

Q15.	Are you aware of your organisations rules about the use of IT resources such as: internet, email and telephones?	
	Yes	45 (70.3%)
	Partially	19 (29.7%)
	No	0 (0.0%)

Q16.	Which of the following are covered by the Data Protection Act if they hold information about a living individual? (please tick all that apply)	
	Electronic information	65 (100.0%)
	Hard copy output	61 (93.8%)
	Handwritten notes	55 (84.6%)
	Audio recordings	58 (89.2%)
	Photographs	58 (89.2%)

Q17.	If your job requires you to share personally identifiable information, how is this shared? (please tick all that apply)	
	Electronically transmitted	26 (54.2%)
	Electronically transmitted - Encrypted	14 (29.2%)
	Electronically transmitted email via secure system (for example GSI)	4 (8.3%)
	By courier mail	9 (18.8%)
	By Recorded delivery	9 (18.8%)
	By Special delivery	8 (16.7%)
	By standard post	10 (20.8%)

Q17.	If your job requires you to share personally identifiable information, how is this shared? (please tick all that apply)	
	Collect or deliver in person	32 (66.7%)

Q18.	Is shared information given a higher level of security if it is sent externally as opposed to internally?	
	Yes	22 (40.7%)
	Sometimes	17 (31.5%)
	No	15 (27.8%)

Q19.	If the information you use every day was incorrectly disclosed, do you think this would be?	
	Low risk - little or no consequence	17 (26.2%)
	Medium risk - limited consequence	43 (66.2%)
	High risk - national consequence	5 (7.7%)

Q20.	If you access work related confidential information when out of the office, how is the information accessed? (Please tick all that apply)	
	On your corporate network (for example Virtual Private Network (VPN))	15 (40.5%)
	Work Laptop/PDA	15 (40.5%)
	Own equipment (for example via web based corporate email site)	8 (21.6%)
	Internet cafe	0 (0.0%)
	Via personal email (for example mailing documents to a private account)	4 (10.8%)
	USB Pen Drive	19 (51.4%)
	Other removable storage (for example CDs, media cards)	8 (21.6%)
	Other	4 (10.8%)

Q21.	You receive a free promotional CD at your work address - what would you do first?	
	Take a look at the contents on your work PC/laptop	14 (22.2%)
	Contact your IT help desk for advice	18 (28.6%)
	Pass it to your line manager/management	9 (14.3%)
	Throw it away	18 (28.6%)
	Take a look at the contents on your home PC/laptop	4 (6.3%)

Q22.	What would you do first if you found a CD on your work desk, and it was labelled:					
		Put it in your PC	Contact your IT help desk	Pass it to your line manager/management	Put it in the bin	Look at it at home
	With your organisation's name/logo?	21 (32.3%)	18 (27.7%)	26 (40.0%)	0 (0.0%)	0 (0.0%)
	Draft Restructuring Plan?	9 (13.8%)	4 (6.2%)	52 (80.0%)	0 (0.0%)	0 (0.0%)
	Department Salary Report?	6 (9.2%)	4 (6.2%)	55 (84.6%)	0 (0.0%)	0 (0.0%)

Q25.	Your computer is destroyed and you are sent a replacement - how would your data be restored?	
	It wouldn't as I hadn't backed it up	4 (6.3%)
	From my own local back-ups	3 (4.7%)
	From the network	47 (73.4%)
	From email attachments	0 (0.0%)
	A mixture of the above	7 (10.9%)
	My data is not critical (doesn't need to be backed up)	3 (4.7%)

Q26.	You find a memory stick (USB flash/pen drive) - What would you do first?	
	Try to find the owner by checking the files on the drive	2 (3.1%)
	Delete the files keep and use for personal use	0 (0.0%)
	Contact your IT help desk	19 (29.2%)
	Ask everyone in the office if they have lost a pen drive	39 (60.0%)
	Leave it at reception	2 (3.1%)
	Pin a notice on your notice board	2 (3.1%)
	Other	1 (1.5%)

Q27.	If you found a memory stick, would you place it in your computer if you…		
		Yes	No
	Found it in the car park?	5 (7.7%)	60 (92.3%)
	Found it in a communal area inside your building?	6 (9.2%)	59 (90.8%)
	Found it on your desk?	12 (18.5%)	53 (81.5%)
	It had your organisations logo on it?	14 (21.5%)	51 (78.5%)
	It was labelled [Your Department Head] Personal files?	2 (3.1%)	63 (96.9%)

Q32.	How would you describe your organisation's IT security?	
	Very good	5 (7.7%)
	Good	24 (36.9%)
	Adequate	32 (49.2%)
	Poor	4 (6.2%)
	Very poor	0 (0.0%)

Q33.	Who is responsible for IT security in your organisation?	
	Everyone	51 (78.5%)
	Central IT	7 (10.8%)
	Dedicated IT security department/personnel	7 (10.8%)
	The board	0 (0.0%)

Q34.	Please indicate which sector you are responding from	
	Local Government	9 (13.8%)
	Health	0 (0.0%)
	Housing	0 (0.0%)
	Community Safety and Cohesion	0 (0.0%)
	Fire and Rescue services	56 (86.2%)

Q35.	Please indicate the option which best describes the area in which you work (LG)	
	Business	0 (0.0%)
	Community and living	0 (0.0%)
	Council, government and democracy	1 (11.1%)
	Education and learning	0 (0.0%)
	Environment	0 (0.0%)
	Health and social care	0 (0.0%)
	Housing	0 (0.0%)
	Jobs and careers	0 (0.0%)
	Legal services	0 (0.0%)
	Leisure and culture	0 (0.0%)
	Policing and public safety	8 (88.9%)
	Social issues	0 (0.0%)
	Transport and streets	0 (0.0%)

If you require a copy of this document in an alternative format or in a language other than English, please call: **0844 798 7070**

Design and production by the Audit Commission Publishing Team.

The Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission explains the respective responsibilities of auditors and of the audited body. Reports prepared by appointed auditors are addressed to non-executive directors, members or officers. They are prepared for the sole use of the audited body. Auditors accept no responsibility to:

- any director/member or officer in their individual capacity; or
- any third party.

Audit Commission

1st Floor
Millbank Tower
Millbank
London
SW1P 4HQ

Telephone: 0844 798 3131
Fax: 0844 798 2945
Textphone (minicom): 0844 798 2946

www.audit-commission.gov.uk November 2010