ITEM NO:5(b)

REPORT TO:	**STANDARDS COMMITTEE**
DATE:	25 November 2014
REPORT OF:	Sandra Stewart – Borough Solicitor (Monitoring Officer)
SUBJECT MATTER:	**INFORMATION GOVERNANCE: ELECTED MEMBER & EMPLOYEE DEVELOPMENT**
REPORT SUMMARY:	The report outlines the training and development programme in place to ensure all employees are appraised of their roles and responsibility in relation to Information Governance
RECOMMENDATION(S)	That the report be noted by Standards Committee.
FINANCIAL IMPLICATIONS: **(Authorised by Borough Treasurer)**	The budget for employee development is included within the Council's overall budget and any costs are funded from this.
LEGAL IMPLICATIONS: **(Authorised by Borough Solicitor)**	The public needs to have confidence that the Council maintains the security of its data. Whilst it is possible to put systems in place, the most important aspect is to ensure that both staff and elected members understand the obligations and liabilities imposed upon them. This report sets out how the Council is ensuring that staff and members are aware of the highest standards that are required to be maintained.
RISK MANAGEMENT:	Ensure that employees are appropriately skilled and aware of the legal obligations to operate within an environment of good information governance.
LINKS TO COMMUNITY PLAN:	Supports the delivery of the Community Strategy by employees across the Borough
ACCESS TO INFORMATION	**NON-CONFIDENTIAL** **This report does not contain information which warrants its consideration in the absence of the Press or members of the public**
REFERENCE DOCUMENTS:	The background papers relating to this report can be inspected by contacting the report writer, Tracy Brennand, Assistant Executive Director (People and Workforce Development): ☎ Telephone:0161 342 3279 ✉ e-mail: tracy.brennand@tameside.gov.uk

1. INTRODUCTION AND BACKGROUND

1.1 In 2013, the Council launched the AGMA E-Learning programme and tools which via the virtual college. This resource is available to all staff within the Council and they can access the e-learning courses available to them. A standard set of courses have been assigned to all staff which include:- Data Protection at Work, Equality and Diversity in the Workplace, Fire Safety and Evacuation, Health and Safety in the Workplace, Responsibility for Information.

2. STAFF TRAINING

2.1 Given the significant importance of Information Governance and the protection of data security, the Council determined that all staff would be required to complete the Data Protection E-Learning course.

2.2 The E-Learning programme covers the fundamental elements of the Data Protection Act and the responsibilities for the safekeeping, sharing, handling and storage of data.

2.3 To date, around 1824 employees have successfully completed the course which equates to approximately 91% of our workforce who have access to computers or personal data records. All remaining employees are expected to have completed their course by the end of December 2014. The table below outlines the completion levels by individual directorate:

Directorate:	Number of users	Completed	Not completed:
Governance	152	152	0
Pensions	140	139	1
Finance	245	238	7
Public Health	39	37	2
People	1122	1011	111
Place	306	247	59
Total	**2004**	**1824**	**180**

2.4 The Council's Senior Management Team have made it clear they regard non-compliance as a breach of disciplinary procedures unless there are exceptional reasons why compliance not achieved for example absent on maternity leave during the relevant period.

2.5 To further reinforce the significance and importance of good information management, particularly in service areas with higher risk levels, the Risk Management service developed a bespoke training programme, which commenced in September 2014.

2.6 Colleagues within Exchequer Services and Children's Services have initially been identified as the priority groups, given the nature of their roles and amount of information that is handled on a daily basis. This is planned for wider engagement with colleagues in Adult Services in the New Year.

2.7 The programme outlines in detail the reason why our staff need to comply with the Data Protection Act and clearly outlines the consequences of non-compliance. In addition, the sessions cover the Information Governance Framework and the application of those requirements in our daily job roles and the individual responsibilities of staff in relation to information handling.

2.8 To date 92 members of staff have attended a bespoke briefing session in addition to them already completing the E-Learning programme on data protection.

2.9 Further sessions are being delivered during November and into the New Year to ensure that employees identified as a priority attend a session. These additional sessions will cover approximately 250 employees, in the main working within Adult Services.

2.10 The online E-Learning programme relating to Information Governance is also being refreshed by colleagues on the AGMA Data Protection Group. Once finalised this will be loaded onto the Virtual College system and all staff will be required to undertake this learning as part of a planned programme of refresher training.

3. MEMBER DEVELOPMENT

3.1 Along with the expectation to engage in a range of specific briefing/development sessions, an essential component has been in relation to Information Governance. A number of sessions have been provided to ensure that Elected Members clearly understand their role and responsibilities in relation to, and in compliance with the:

- Data Protection Act
- Human Rights Act,
- Common Law Duty of Confidentiality; and
- Code of Conduct for Councillors.

3.2 These sessions enabled Elected Members to consider and address specific situational examples that were directly relevant to the nature of their role as an Elected Member and were guided by the Information Commissioners Officer (ICO) Good Practice Advice for both elected and prospective members of local authorities.

3.3 The briefing sessions also outlined in detail the security actions that are essential to ensure that Elected Members operate and use portable electronic devices, paper documents and removable media safely and securely.

3.4 The briefing sessions have been received very positively by Elected Members and have, for example enabled them to clarify specific issues that are often raised by their constituents in relation to the requirement for them to request permission of the resident if passing on personal details to other ward colleagues.

3.5 Two sessions have already been delivered to 16 Elected Members with a further session for 13 Elected Members planned for 1 December 2014. A further session to accommodate those who have not been able to attend the earlier sessions has been arranged for January 2015. A copy of the presentational material is set out at **Appendix 1.**

3.6 Social media is an extremely useful tool for Elected Members to enable them to keep in touch with their constituents as well as to keep abreast of developments and current issues within the Borough. In addition to this Social media can be used as an informative tool to bolster a Members Election campaign. Consequently, social media training was made available to those Members who were interested in learning details of the different and varied platforms (Facebook and Twitter) available.

3.7 Social Media training has been provided during 2014 to those Members who are unfamiliar with the different social networks available. In addition to this, Members who already use the platforms have been provided with advice and support to ensure they keep themselves safe whilst online, as well as learning the potentials risks and outcomes of comments that are made online for both the Council and themselves personally.

Information Governance

Peter Wilson

Tameside Metropolitan Borough

What is Information Governance?

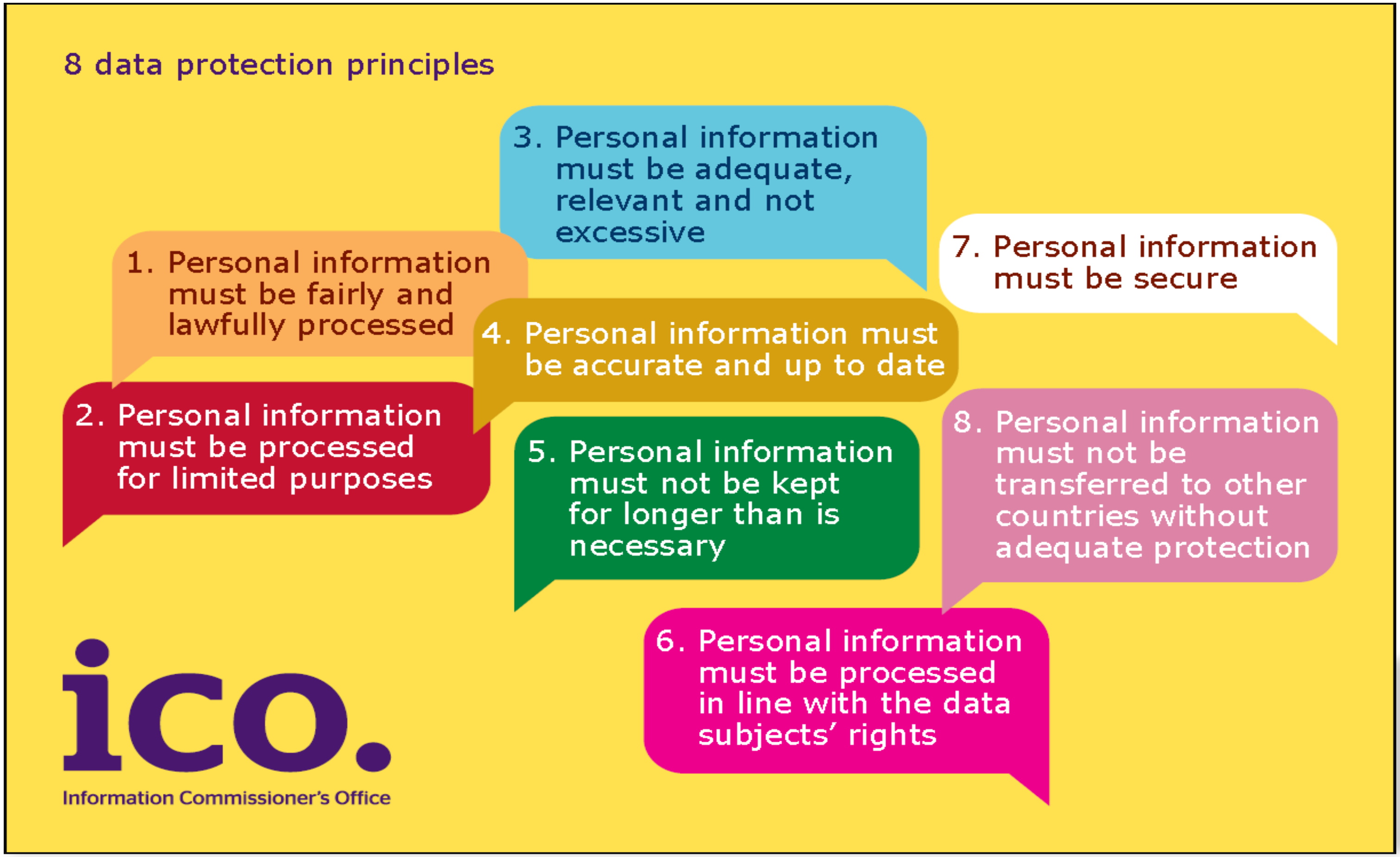
Information governance is the term used to describe the principles, processes and legal and ethical responsibilities for managing and handling information.

It sets the requirements and standards that organisations need to achieve to ensure that information is handled legally, securely, efficiently and effectively.

How does it affect me?

- All organisations are required to comply with the requirements of the Data Protection Act 1998.
- The Information Commissioner's Office enforces the requirements of the Data Protection Act 1998.
- Breaches of the Data Protection Act can incur fines of up to £500,000 and Personal Fines up to £50,000.
- As members you have all signed the Code of Conduct, which requires you to treat information securely and appropriately.

The Data Protection Principles



8 data protection principles

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection

ico.

Information Commissioner's Office

Responsibilities

Whilst dealing with constituent queries members will be required to comply with the requirements of the Data Protection Act 1998, Human Rights Act 1998 and the Common Law Duty of Confidentiality. Along with the requirements of the Code of Conduct.

<u>This applies to both:</u>

- The information provided to you by the Resident (data subject).

&

- The information (answer) provided to you by the Council.

The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002

- If you are handling a query on behalf of a resident (data subject) in your ward you will be technically “processing” the information provided.

- The Council is allowed to provide elected members with information when it is in connection with the discharge of their functions as an elected representative.

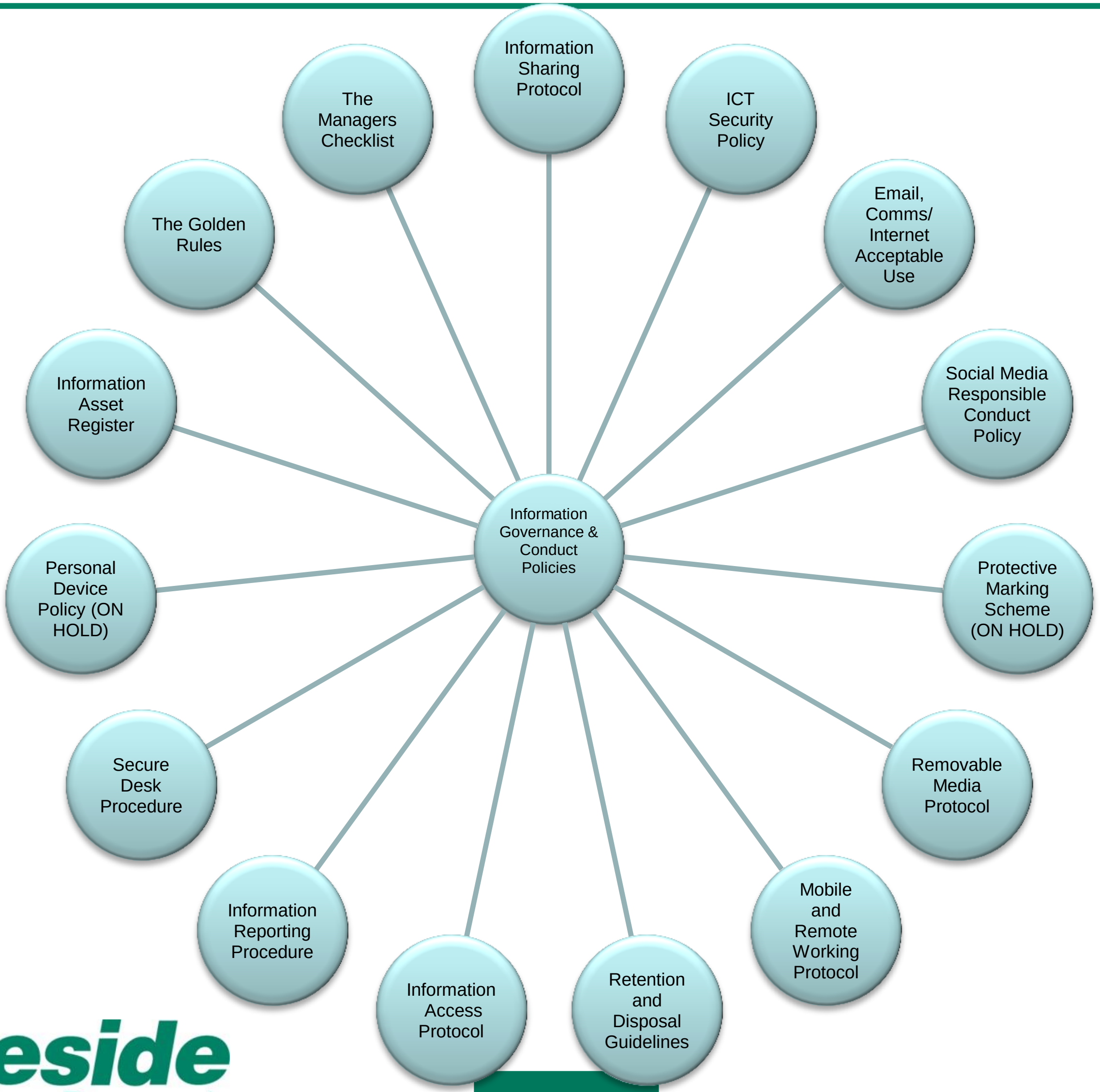
Tameside
Metropolitan Borough

Responsibilities

- Transporting the information securely.
- Keeping the records of the query safely.
- Discussions about the query do not involve those that do not need to know.
- Providing the answer to the resident.
- When the information is no longer needed, disposing of it securely.

Tameside Metropolitan Borough

Information Risk What Are We Doing?



Information Governance & Conduct Policies

Information Sharing Protocol

ICT Security Policy

Email, Comms/ Internet Acceptable Use

Social Media Responsible Conduct Policy

Protective Marking Scheme (ON HOLD)

Removable Media Protocol

Mobile and Remote Working Protocol

Retention and Disposal Guidelines

Information Access Protocol

Information Reporting Procedure

Secure Desk Procedure

Personal Device Policy (ON HOLD)

Information Asset Register

The Golden Rules

The Managers Checklist

Tameside Metropolitan Borough

Information Governance

- Members are accountable and owe a duty of care to the Council, service users and the residents of Tameside, who they act on behalf of and whose information they handle. This is set out in the Code of Conduct, which all members have signed.

- It is the responsibility of all members to ensure their use of personal or sensitive information does not breach the requirements of the Data Protection Act 1998 or any other applicable legislation.

What the ICO thinks……

Information Commissioner Christopher Graham said:

> “It would be far too easy to consider these breaches as **simple human error**. The reality is that they are caused by councils treating sensitive personal data in the same routine way they would deal with more general correspondence. Far too often in these cases, the councils do not appear to have acknowledged that the data they are handling is about real people, and often the more vulnerable members of society.”

“IT WAS HUMAN ERROR” IS NOT AN EXCUSE!

Information Governance – Portable Devices

- Portable devices (iPads/laptops) must be secured when not in use.

- When creating a password, you should not select a password that can easily be deduced by others; in particular, you should not use passwords which are easy to guess (e.g. the names of partner children or pets). It is advisable to use a mix of characters, e.g. three out of four of: upper or lower case alphabetic characters, numbers and symbols in each password.

You can check your password strength here:

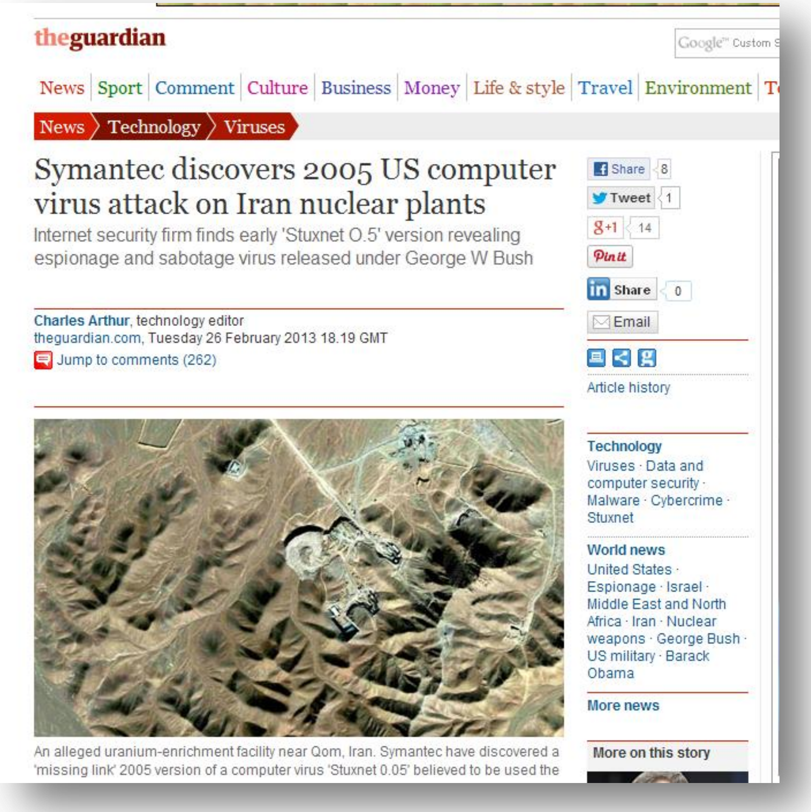
https://www.grc.com/haystack.htm (external website)

Tameside Metropolitan Borough

Removable Media Protocol

- Removable media refers to devices that are used to store or transport data.
- Removable media which is not owned by the Council must not normally be connected to Council owned equipment.
- As set out in the ICT Security Policy, only encrypted USB memory sticks purchased through ICT Services may be used in the Council.
- Any non encrypted device connected to the Council’s network will not be permitted to download information onto it and a message will be displayed by the monitoring software.
- In order to minimise physical risk such as loss or theft, all removable media must be stored in an appropriately secure and safe environment when not in use (e.g. locked cupboard or drawer).

Virus spreading



theguardian

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment | T

News › Technology › Viruses

Symantec discovers 2005 US computer virus attack on Iran nuclear plants

Internet security firm finds early 'Stuxnet 0.5' version revealing espionage and sabotage virus released under George W Bush

Charles Arthur, technology editor
theguardian.com, Tuesday 26 February 2013 18.19 GMT
Jump to comments (262)

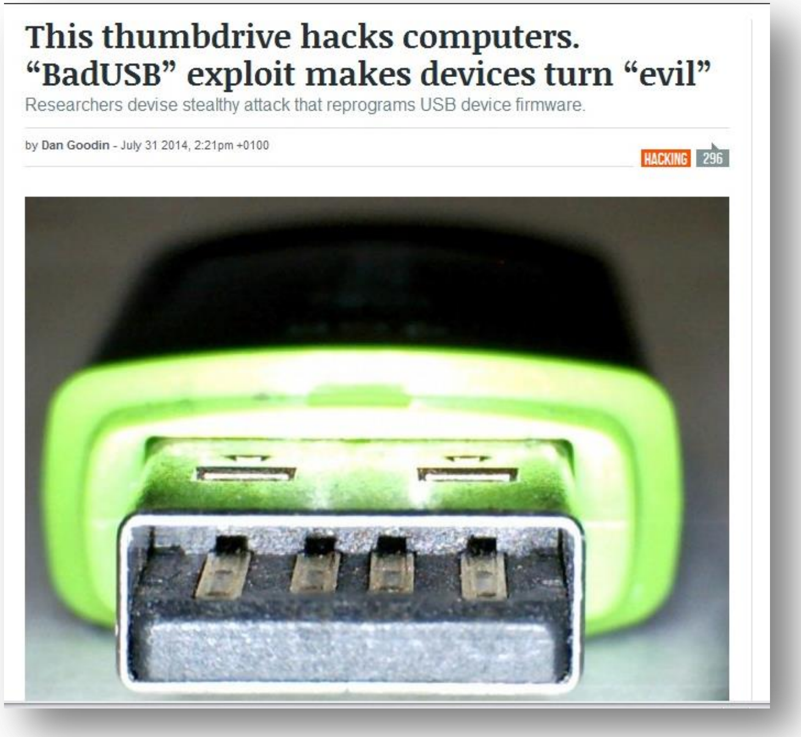
Share 8
Tweet 1
g+1 14
Pin it
in Share 0
Email
Article history

Technology
Viruses · Data and computer security · Malware · Cybercrime · Stuxnet
World news
United States · Espionage · Israel · Middle East and North Africa · Iran · Nuclear weapons · George Bush · US military · Barack Obama
More news
More on this story

An alleged uranium-enrichment facility near Qom, Iran. Symantec have discovered a 'missing link' 2005 version of a computer virus 'Stuxnet 0.05' believed to be used the

The 1.0 version of Stuxnet is reckoned to have infected Iranian computers
after being copied onto USB memory sticks
which were left in locations in India and Iran known to be used
by Iranian nuclear scientists and their contacts.

New Issues



This thumbdrive hacks computers. “BadUSB” exploit makes devices turn “evil”

Researchers devise stealthy attack that reprograms USB device firmware.

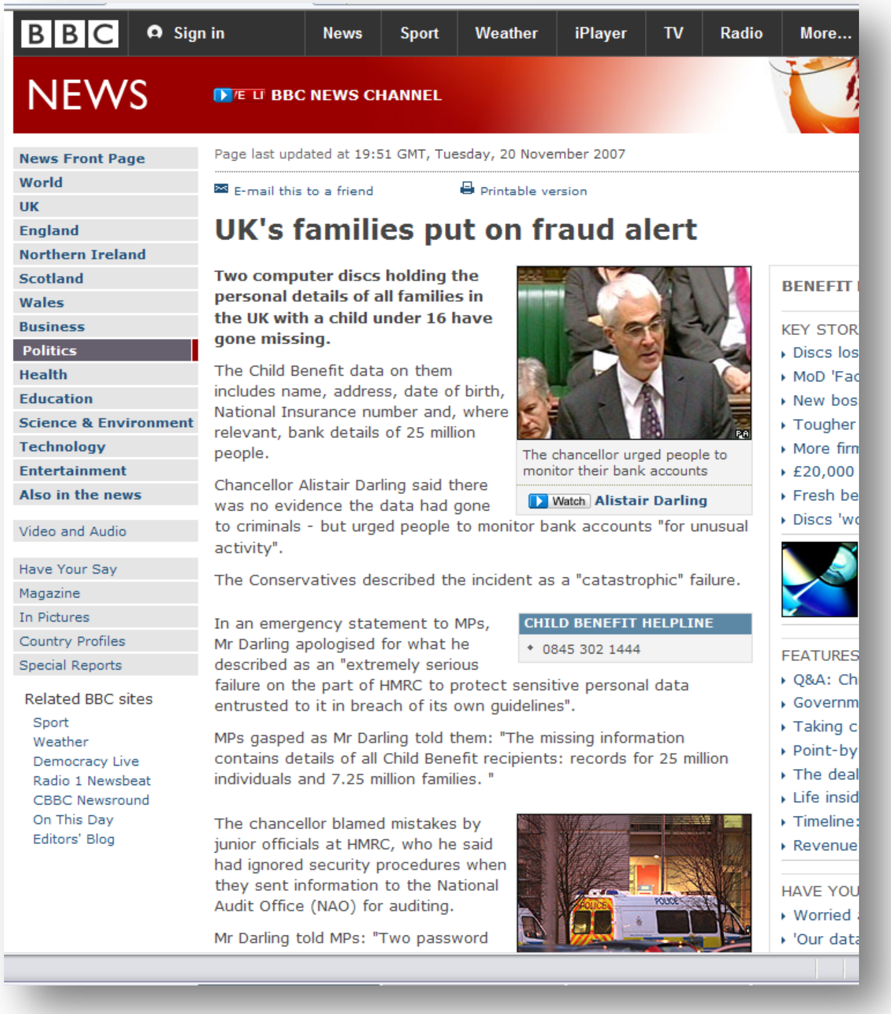
by Dan Goodin - July 31 2014, 2:21pm +0100

Dubbed BadUSB, the hack reprograms embedded firmware to give USB devices new, covert capabilities.
A USB memory stick, will take on the ability to act as a keyboard that surreptitiously types malicious commands into attached computers.

Removable Media Protocol

- It is essential that all removable media is disposed of securely to minimise the risk of the accidental disclosure of sensitive information. All ICT equipment (e.g. USB memory sticks, hard drives etc) that are surplus to requirements or have become damaged must be returned to ICT Services.
- Removable media devices associated with mobile phones (SIM cards, memory cards etc) should be returned to Media, Marketing and Communications along with the relevant device to ensure any data is removed from the handset before reallocation/disposal.

HMRC Loses data on 25 million people.



Page last updated at 19:51 GMT, Tuesday, 20 November 2007

UK's families put on fraud alert

Two computer discs holding the personal details of all families in the UK with a child under 16 have gone missing.

The Child Benefit data on them includes name, address, date of birth, National Insurance number and, where relevant, bank details of 25 million people.

The chancellor urged people to monitor their bank accounts

Watch Alistair Darling

Chancellor Alistair Darling said there was no evidence the data had gone to criminals - but urged people to monitor bank accounts "for unusual activity".

The Conservatives described the incident as a "catastrophic" failure.

CHILD BENEFIT HELPLINE

- 0845 302 1444

In an emergency statement to MPs, Mr Darling apologised for what he described as an "extremely serious failure on the part of HMRC to protect sensitive personal data entrusted to it in breach of its own guidelines".

MPs gasped as Mr Darling told them: "The missing information contains details of all Child Benefit recipients: records for 25 million individuals and 7.25 million families. "

The chancellor blamed mistakes by junior officials at HMRC, who he said had ignored security procedures when they sent information to the National Audit Office (NAO) for auditing.

Mr Darling told MPs: "Two password

Council lost memory stick containing 18,000 residents' details

Rochdale Metropolitan Borough Council breached the Data Protection Act by losing an unencrypted memory stick containing the details of over 18,000 residents.

The memory stick – which was lost in May 2011 and has not been recovered – included, in some cases, residents' names and addresses, along with details of payments to and by the council. The information had been put on a memory stick to compile the council's financial accounts.

The ICO's investigation found that the council's data protection practices were insufficient – specifically that it failed to make sure that memory sticks provided to its staff were encrypted.

Information Governance - Email Risks

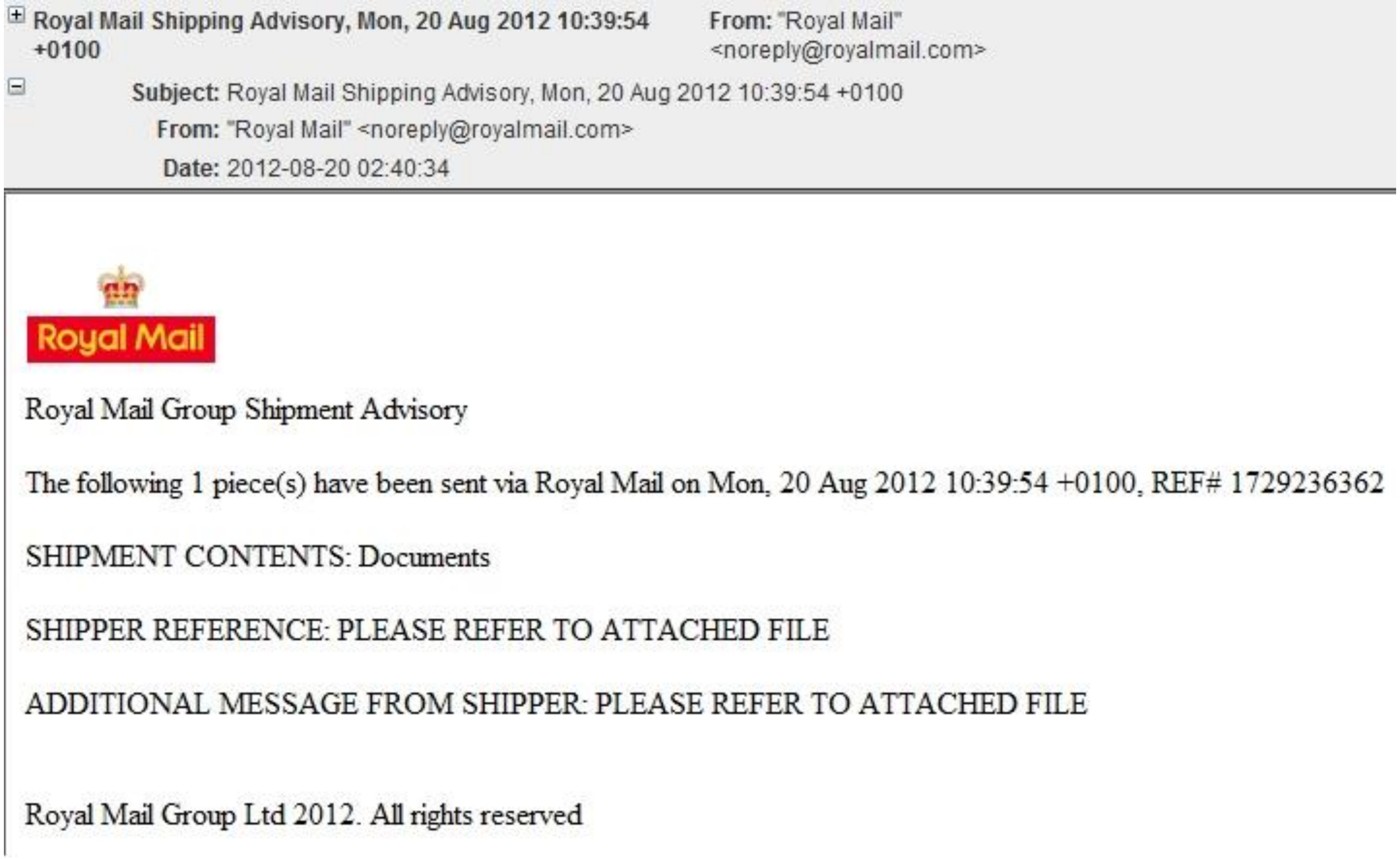
- It is important to remember that an email sent outside the “tameside.gov.uk” network, over the internet is not secure. Unless you are using a GCSX account. You should not therefore send any private or confidential information by external email unless it is properly encrypted.
- This can be done using 7-Zip, by encrypting and password protecting a document.
- You should note that there are a number of inherent risks involved in using the internet, particularly a lack of confidentiality when transmitting information. This is why you should let the recipient know the password separately.

Information Governance – Virus Transmission

- Computer viruses have the potential to cause enormous damage to Systems and the data they hold. ANY disk or memory stick being brought into the Council should be virus checked before loading.

- Viruses may be transmitted through E-mails and/or attachments. If anyone has any doubt about an e-mail received, especially from an unknown source, refer it to the IT Helpdesk. Do not open any suspicious e-mail or attachment.

Malicious Emails



⊞ Royal Mail Shipping Advisory, Mon, 20 Aug 2012 10:39:54 +0100 — From: "Royal Mail" <noreply@royalmail.com>

⊟ **Subject:** Royal Mail Shipping Advisory, Mon, 20 Aug 2012 10:39:54 +0100

From: "Royal Mail" <noreply@royalmail.com>

Date: 2012-08-20 02:40:34

Royal Mail Group Shipment Advisory

The following 1 piece(s) have been sent via Royal Mail on Mon, 20 Aug 2012 10:39:54 +0100, REF# 1729236362

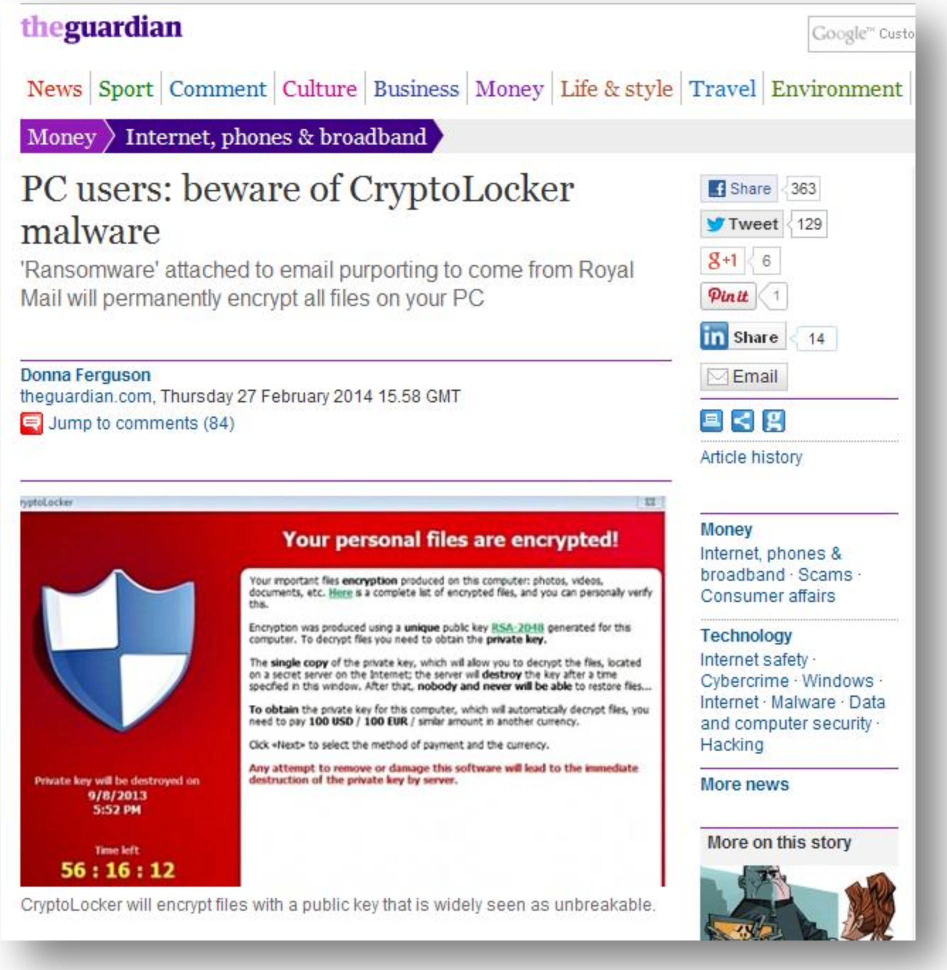
SHIPMENT CONTENTS: Documents

SHIPPER REFERENCE: PLEASE REFER TO ATTACHED FILE

ADDITIONAL MESSAGE FROM SHIPPER: PLEASE REFER TO ATTACHED FILE

Royal Mail Group Ltd 2012. All rights reserved

Risks on the Web.


theguardian
Google™ Custo
News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment
Money › Internet, phones & broadband
Share 363
Tweet 129
g+1 6
Pin it 1
in Share 14
Email
Article history
Money
Internet, phones & broadband · Scams · Consumer affairs
Technology
Internet safety · Cybercrime · Windows · Internet · Malware · Data and computer security · Hacking
More news
More on this story

PC users: beware of CryptoLocker malware

'Ransomware' attached to email purporting to come from Royal Mail will permanently encrypt all files on your PC

Donna Ferguson
theguardian.com, Thursday 27 February 2014 15.58 GMT
Jump to comments (84)

yptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

CryptoLocker will encrypt files with a public key that is widely seen as unbreakable.

Malware can be downloaded from websites or email links.

The latest form of this is “Ransomware”

Information Governance - Social Media

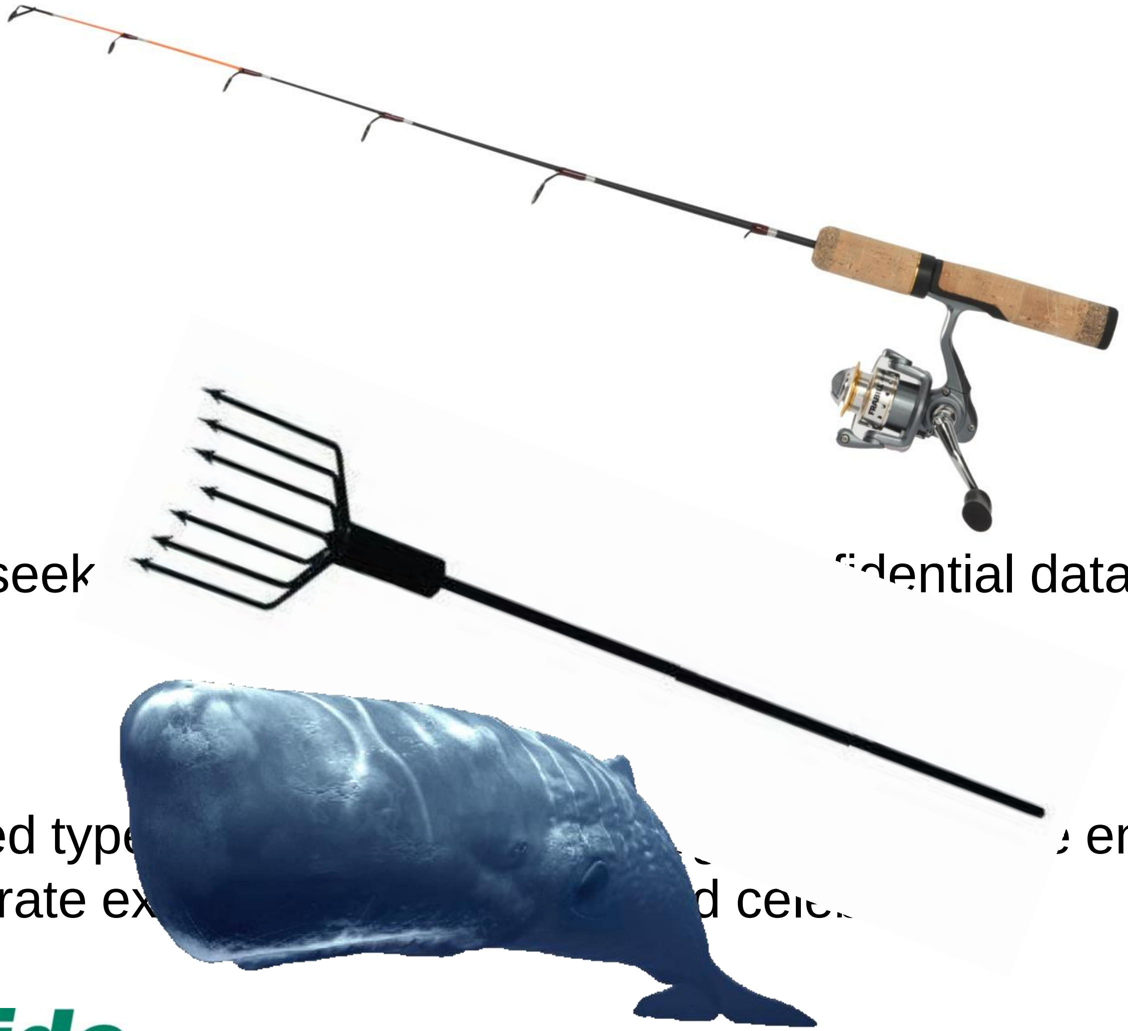
- Social networking websites ….allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.
- Being security conscious and taking steps to protect yourself from identity theft or account hacking by restricting the amount of personal information you share on the internet is important.
- Ensure no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information belonging to the Council, other councillors and/or members of the public.

Quick Quiz

- Phishing –
- The frauduler
  reputable com rsonal
  information, s e.

- Spear Phishir
- Similar to phis cific
  organisation, seek idential data.

- Whaling –
- A more focused typ end users
  such as corporate ex d cele

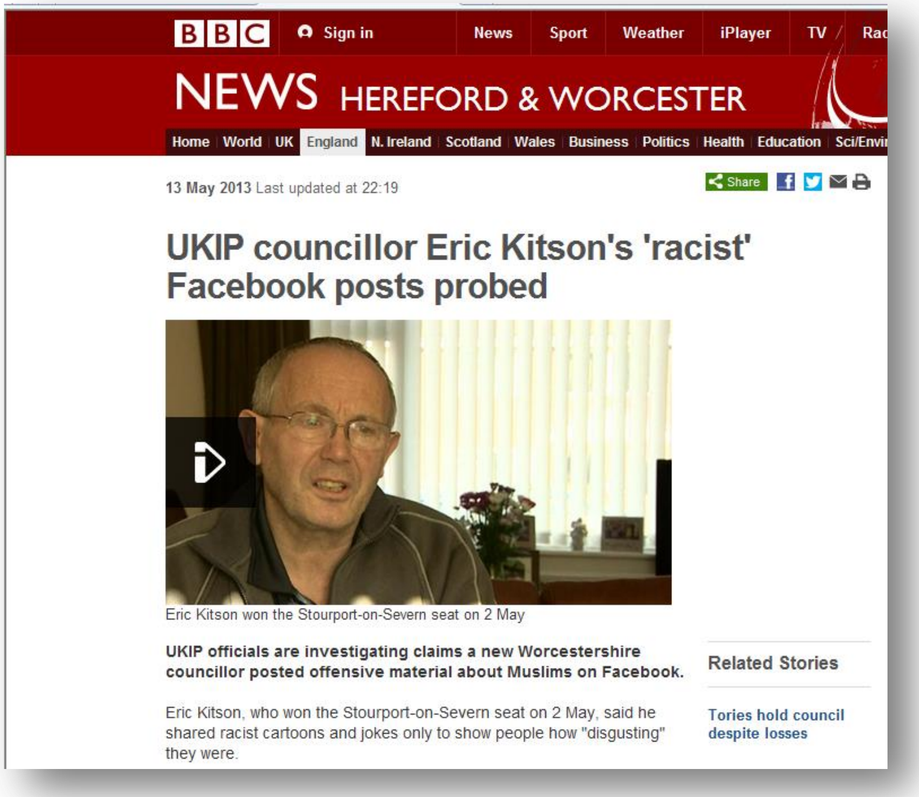


Information Governance - Social Media

- You must stay within the law at all times. Be aware that fair use, financial disclosure, libel, defamation, copyright and data protection laws apply on-line just as in any other media.

- Remember your obligations to residents, service users, partners, suppliers and colleagues. Never give out details of or divulge dealings with colleagues, customers or partners without their explicit consent.

Social Media…The Worldwide Conversation



13 May 2013 Last updated at 22:19

UKIP councillor Eric Kitson's 'racist' Facebook posts probed

Eric Kitson won the Stourport-on-Severn seat on 2 May

UKIP officials are investigating claims a new Worcestershire councillor posted offensive material about Muslims on Facebook.

Eric Kitson, who won the Stourport-on-Severn seat on 2 May, said he shared racist cartoons and jokes only to show people how "disgusting" they were.

Related Stories

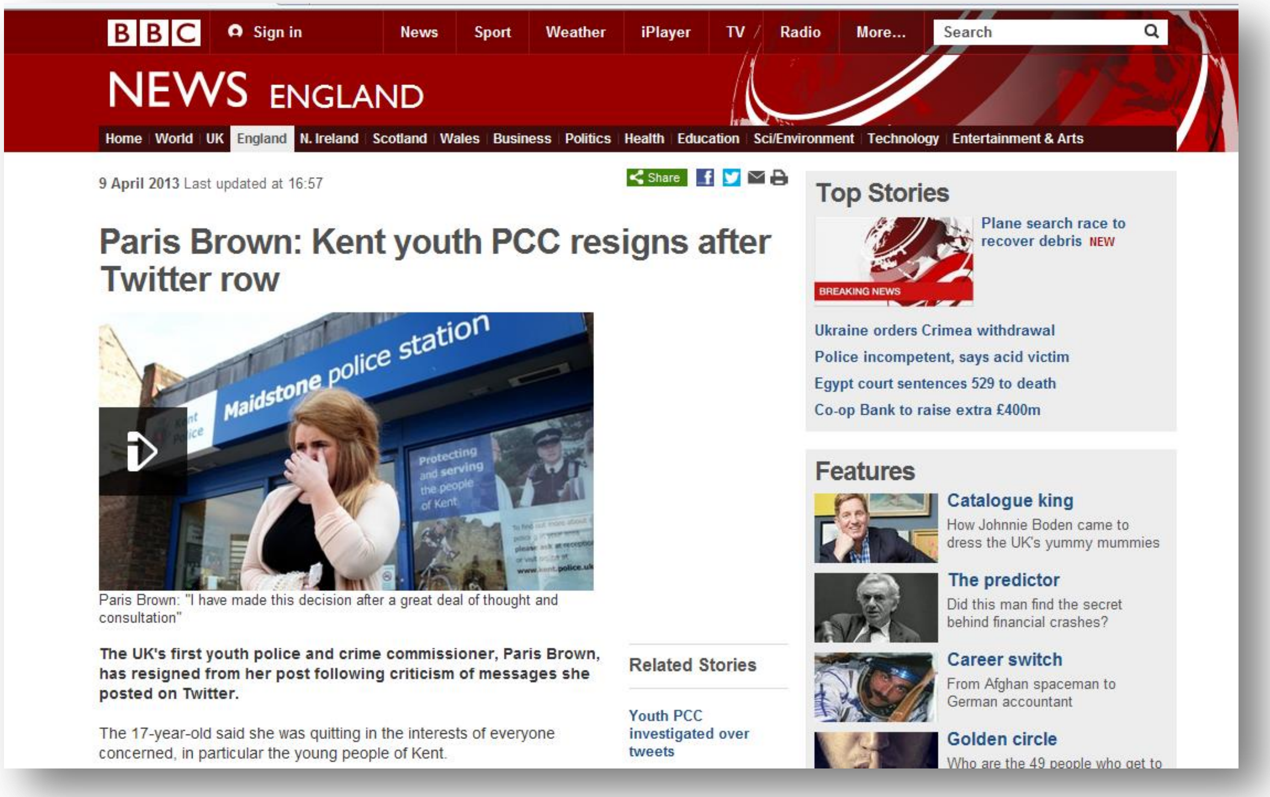
Tories hold council despite losses

Eric Kitson, shared racist cartoons and jokes only to show people how "disgusting" they were.

He said it had been "stupid" for him to share the messages.

He has shut his Facebook account and said he was considering resigning.

Social Media….is around for a long time



9 April 2013 Last updated at 16:57

Paris Brown: Kent youth PCC resigns after Twitter row

Paris Brown: "I have made this decision after a great deal of thought and consultation"

The UK's first youth police and crime commissioner, Paris Brown, has resigned from her post following criticism of messages she posted on Twitter.

The 17-year-old said she was quitting in the interests of everyone concerned, in particular the young people of Kent.

Related Stories

Youth PCC investigated over tweets

Top Stories

Plane search race to recover debris NEW

Ukraine orders Crimea withdrawal

Police incompetent, says acid victim

Egypt court sentences 529 to death

Co-op Bank to raise extra £400m

Features

Catalogue king
How Johnnie Boden came to dress the UK's yummy mummies

The predictor
Did this man find the secret behind financial crashes?

Career switch
From Afghan spaceman to German accountant

Golden circle
Who are the 49 people who get to

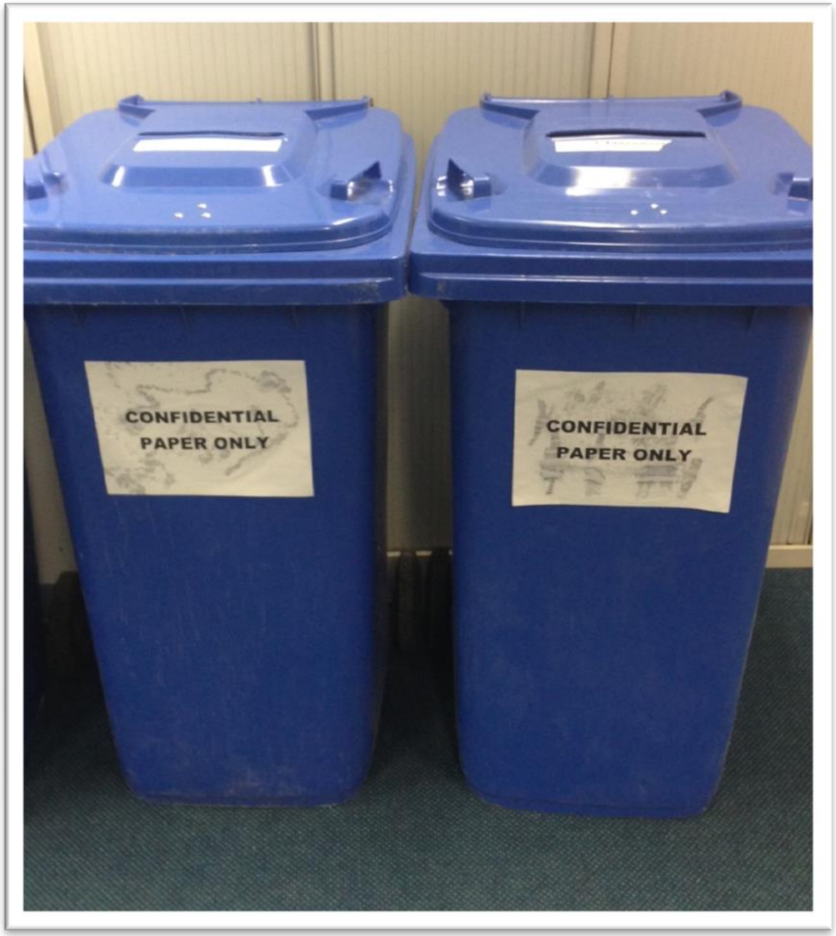
Mobile and Remote Working Protocol.

- Any equipment supplied by the Council may only be used by authorised persons.
- Portable devices (iPads/laptops) issued by the Council are usually insured when they are inside the United Kingdom, although misuse or inadequate protection may invalidate that insurance cover.
- All protected information (including information stored on portable devices and in paper files) must not be left where it would attract the interest of an opportunist thief.
- Protected information must be located securely and out of sight so that visitors or family members do not have access.
- Ensure that any telephone conversations discussing protected information cannot be overheard.

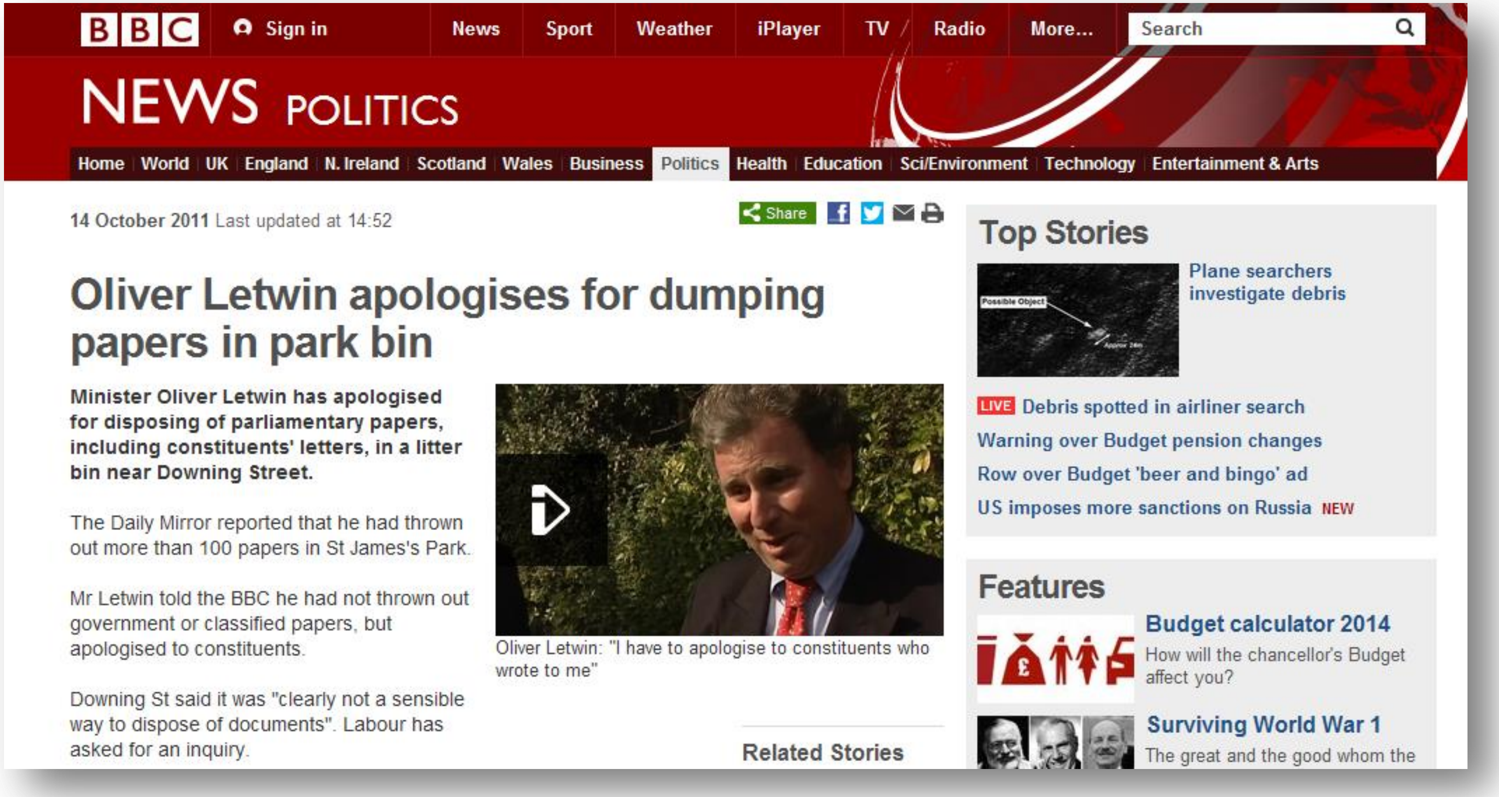
Mobile and Remote Working Protocol.

- When working out of the office, members should not be using externally provided WiFi Hotspots or free WiFi connections provided by retail outlets, coffee shops and the like, when dealing with personal or sensitive information.
- The only exception to this would be a private network that requires a password to access. For example WiFi at another Local Authority building, or at a business or academic premises. Purchased connectivity at a hotel, where you are given a unique password would also be acceptable.
- Any information that would qualify as being personal or sensitive must be returned to the Council office and disposed of in the blue security bins or shredded.

Use the Confidential Waste Bins



Does it really effect me?



14 October 2011 Last updated at 14:52

Oliver Letwin apologises for dumping papers in park bin

Minister Oliver Letwin has apologised for disposing of parliamentary papers, including constituents' letters, in a litter bin near Downing Street.

The Daily Mirror reported that he had thrown out more than 100 papers in St James's Park.

Mr Letwin told the BBC he had not thrown out government or classified papers, but apologised to constituents.

Downing St said it was "clearly not a sensible way to dispose of documents". Labour has asked for an inquiry.

Oliver Letwin: "I have to apologise to constituents who wrote to me"

Related Stories

Top Stories

Plane searchers investigate debris

LIVE Debris spotted in airliner search

Warning over Budget pension changes

Row over Budget 'beer and bingo' ad

US imposes more sanctions on Russia NEW

Features

Budget calculator 2014

How will the chancellor's Budget affect you?

Surviving World War 1

The great and the good whom the

Data Protection Good Practice Note Information Commissioner’s Office

Advice to local authorities on disclosing personal information to elected members V2.0

Disclosures to the elected member as a member of the council

- Local authorities can disclose personal information to an elected member if they need to access and use that information to carry out official duties.

  Example *: A member of the Housing Committee may attend a meeting to decide whether or not to seek the eviction of a council tenant. The local authority may provide them all the relevant personal information about the tenant and the circumstances giving rise to the possible eviction. However, the local authority would not be justified in providing the elected member with general access to the Housing Department system.*

Data Protection Good Practice Note Information Commissioner's Office

Disclosures to elected members acting on behalf of local residents

A local authority does not generally have to get the consent of an individual to disclose their personal information to an elected member, as long as:

- the elected member represents the ward in which the individual lives;
- the elected member makes it clear that they are representing the individual in any request for their personal information to the local authority;
- and the information is necessary to respond to the individual's complaint.

Where personal information is particularly sensitive, it may be advisable to get an individual's signed consent.

Data Protection Good Practice Note Information Commissioner’s Office

Disclosures to elected members for political purposes

Local Authorities should not normally disclose personal information to elected members for political purposes without the consent of the individuals concerned.

There are two exceptions to this:

- There may be sets of personal information which the local authority is required to make public, for example, lists of some types of licence holder.
- Personal information may also be disclosed if it is presented in an aggregated form and does not identify any living individuals, for example, Council Tax band information or statistical information.

However, there would be a breach of the Act if personal information was released in an apparently anonymised form which could then be linked to the individuals concerned, for example, by comparing property data with the electoral roll.

Personally Fine or Personally Fined?

Barclays Bank employee prosecuted for illegally accessing customer’s account

The employee was **fined £3,360** after illegally accessing the details of a customer’s account. In one case the employee, Jennifer Addo, found out the number of children the customer had and passed the details to the customer’s then partner, who was a friend of Ms Addo.

Ms Addo was prosecuted under section 55 of the Data Protection Act and fined £2,990 for 23 offences and ordered to pay a £120 victim surcharge and £250 prosecution costs.

Example 1

Example	Bad Practice ✗	Good Practice ✓
An elected member helps a constituent with a particular issue and wishes to use the constituent’s personal information to progress a party political matter on the same issue.	The elected member uses the constituent’s personal information without their consent.	The elected member seeks the consent of the constituent before using their personal information.

Data Protection Good Practice Note Advice for the elected and prospective members of local authorities V2.0

Example 2

Example	Bad Practice ✗	Good Practice ✓
A resident asks one elected member for help with a noisy neighbour.	The elected member does not tell the complainant that he intends to give their personal information to another ward colleague and goes ahead anyway. The resident finds out and makes a complaint.	The member lets the resident know he intends to give their personal information to another ward colleague because that particular councillor has knowledge and experience with this subject. If the constituent objects, he does not disclose the information.

Data Protection Good Practice Note Advice for the elected and prospective members of local authorities V2.0

Example 3

Example	Bad Practice ✗	Good Practice ✓
A resident asks one of their elected members in a multi-member ward for help about teenagers acting in an intimidating way in the area. The elected member wishes to share the constituent's complaint with the other members of the ward because it is an issue of general concern.	The elected member does not inform the constituent that they intend to give the details of their particular complaint to the other ward colleagues and releases the information. The resident finds out and is afraid of reprisals if the information they have leaks out.	The elected member lets the constituent know that he wants to give the details of their complaint to the other ward councillors and why he wants to do that rather than giving a general description of the complaint to other ward members. If the constituent objects, then their wishes are respected and only the general nature of the complaint is shared.

What Next?

Paper Documents containing personal/confidential information.

- Transport in a secure bag, one which can be closed fully and preferably lockable.
- Once used dispose of them securely in the blue confidential waste bins.
- Consider the content of any letters or documents when sending via standard post.
- When at home secure paperwork out of sight in a drawer or cabinet when not needed.

What Next?

Portable devices containing personal/confidential information.

- Always lock away in the boot of your vehicle when transporting.
- Be aware of “shoulder surfers” when using public transport.
- Do not use free or non password access WiFi when working outside Council buildings.
- Ensure your password is strong.

What Next?

Removable Media.

- Only use encrypted memory sticks supplied by ICT.
- Avoid connecting non Council issued memory sticks to the network.
- Delete information off memory sticks when no longer needed.

What Next?

Email usage.

- Sending emails outside of the TMBC network is not secure.
- Ensure email addresses are typed in correctly.
- If sending emails containing personal or confidential information outside of the network, zip, encrypt and password protect the content.
- Emails are still subject to the FOIA and subject access requests under the Data Protection Act.

What Next?

Social Media usage.

- Be conscious of the level of information disclosed.
- Once published it will be there for years to come.
- Consider how others would view your published comments or pictures.
- Would the content you publish breach you Code of Conduct responsibilities?
- Despite security settings, content can be copied and downloaded and reused.

What Next?

Access to information.

- Council information can be disclosed to members for carrying out their official duties.
- The use of personal/confidential information requires permission.
- Permission is required for the sharing of personal or confidential information.
- If in doubt seek advice from the Head of Democratic Services or the Executive Director (Governance)

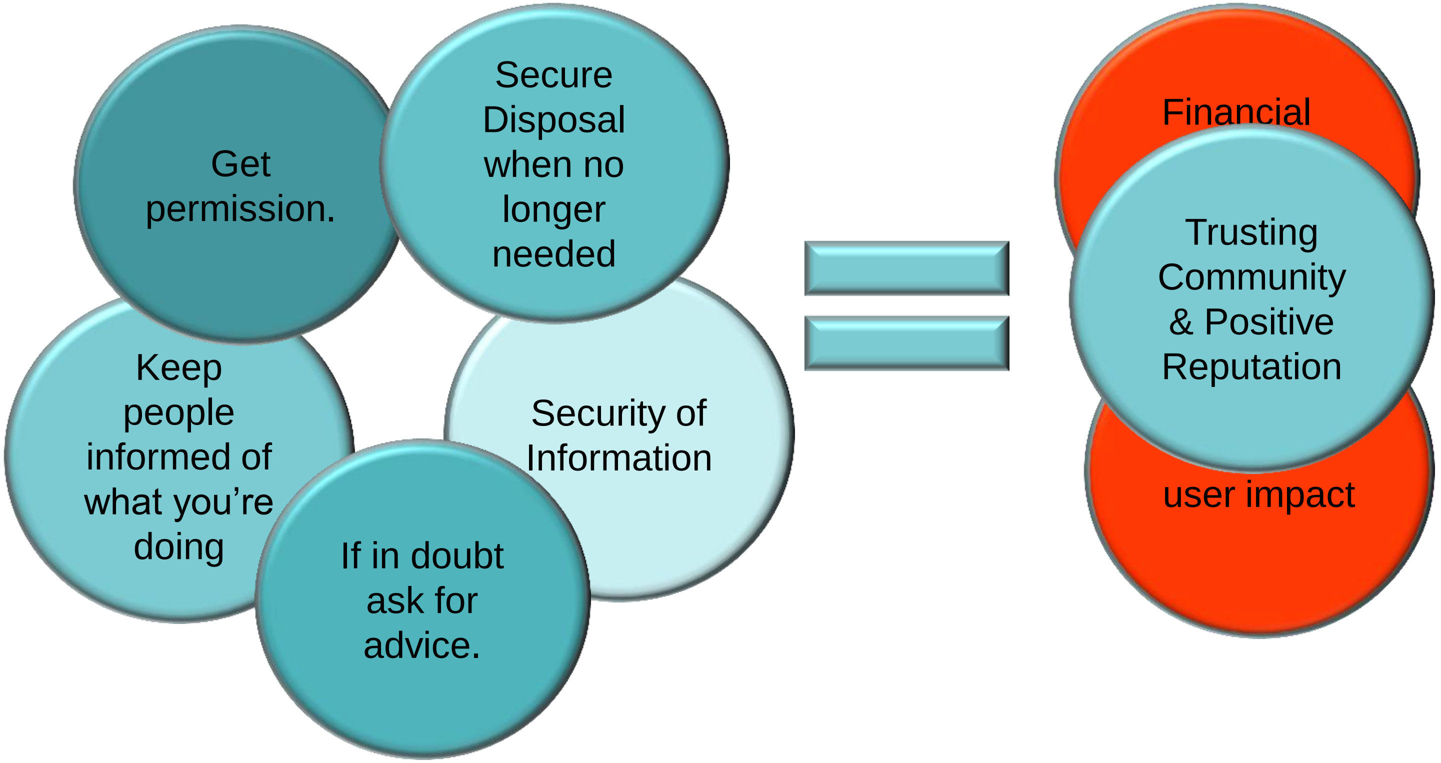
What the ICO thinks…….

“No public service organisation can ever say it will not lose information - but by ensuring the standards in your organisation are equivalent to, or exceed, the best practice identified…..the public and the Information Commissioner’s Office (ICO) will be reassured that all reasonable steps were taken to preserve and protect their personal information”.

Local Public Services Data Handling Guidelines Version 2 August 2012

Responsibilities

Summary



Get permission.

Secure Disposal when no longer needed

Keep people informed of what you're doing

Security of Information

If in doubt ask for advice.

Financial

Trusting Community & Positive Reputation

user impact

Tameside Metropolitan Borough

Questions

Thank you for listening

Do you have any questions?

Tameside Metropolitan Borough