BARNSLEY METROPOLITAN BOROUGH COUNCIL

This matter is not a Key Decision within the Council's definition and has not been included in the relevant Forward Plan

Joint Report of the Executive Directors of Core and Communities

MEMBERS INFORMATION GOVERNANCE AND SECURITY SUPPORT

1. Purpose of report

The purpose of this report is to provide Cabinet with an overview of the support options available to Elected Members with regard to information governance and seek approval to progress with the recommendations.

2. Recommendations

It is recommended that:

2.1 Elected Members adopt the Council's policies and procedures for information governance and security; and

2.2 Elected Members undertake the Council's mandatory annual training for information governance and security, that incorporates undertaking an assessment and can demonstrate good knowledge, awareness and compliance to meet ongoing legislation requirements.

3. Introduction

3.1 During October 2015, the Information Commissioners Office (ICO) took the decision that Elected Members across the country would need to be individually registered as data controllers for the information they handle when working with constituents.

3.2 The Council arranged for each Elected Member to be registered with ICO.

3.3 Many Elected Members obtain personal data, which enables them to carry out casework on behalf of their constituents, examples of personal data captured but not limited to include; names, addresses, family, lifestyle and social circumstances, financial information, education and employment details, housing information and specifics around complaints.

3.4 In addition to 3.3, Elected Members may also obtain sensitive information on behalf of their constituents such as physical or mental health details, trade union membership, racial or ethnic origin, offences including alleged offences and the political affiliation of members.

3.5 Elected Members in order to undertake their community duties and responsibilities effectively are required to share personal and sensitive information with elected representatives and other holders of public office, landlords, local and central government, statutory law enforcement agencies and investigating bodies, political organisations, the media, healthcare, social and welfare practitioners, suppliers and the subject matters of complaints.

3.6 As a data controller, Elected Members are required by law to observe and comply with the key principles for processing personal information; the Data Protection Act 1998. Given that Members' roles require them to share information with the parties mentioned above, Elected Members may have an increased risk of breaching the Act if data is not properly processed.

3.7 The Data Protection Act 1998 is currently under review, with the newly launched General Data Protection Regulations coming into force on 25th May 2018. These new regulations introduce further rigorous controls that all data controllers must fully comply with.

3.8 The Council's Information Governance service is progressing well with implementing the changes required of the new Legislation across all Directorates. However, these requirements apply equally to Elected Members and, as data controllers, they must also be able to demonstrate compliance in the way they handle personal and sensitive information, in addition to the steps taken by the Council as an organisation.

3.9 ICO can and indeed have imposed fines on data controllers of up to £500,000 for a serious breach of the Data Protection Act. It is therefore vital that all personal and sensitive information is handled within the requirements of the law.

3.10 Changes in the new Legislation sanction the ICO to increase fines up to €20M or 4% annual turnover. These fines include prosecuting data controllers who have ignored changes to the Act and not implemented the new process and procedural controls. ICO expects all data controllers to demonstrate their compliance, applying zero tolerance to any exceptions.

3.11 What seems like a simple mistake can have substantial consequences to the person whose data has been violated. The fines imposed by the ICO demonstrate the significance of understanding Elected Member responsibilities, detailed within Appendix A - Examples of ICO Imposed Fines.

4. Proposal and justification

4.1 It is proposed that Elected Members follow as a minimum existing Council processes for information governance and security including those for the purpose of education and awareness. A mandatory Information Management, Governance and Security course and assessment has recently been undertaken by all of the Councils network users. This is a prerequisite for accessing the Council's computer network using a Council device.

4.2 This core offer is extended to Elected Members with specific tailored training familiarisation sessions based on the content of the course referenced in 4.1, which will meet the minimum training and awareness requirements, and be facilitated by the Member Support team. The content will include how the Legislation applies to Elected Members in their role of Councillor and include best practice guidance, and arrangements for receiving, recording, holding, disclosing and securely disposing of information. It also includes how to recognise spoof / phishing emails and records management.

5. Consideration of alternative approaches

5.1 Option 1 – Elected Members manage their own Data Protection compliance

This option would require Elected Members to draft and implement their own policies and procedures demonstrating compliance and understanding of the Legislation. After the Council's recent consultation with the ICO, the ICO recommend this option for all data controllers however the Council appreciates that this is a huge undertaking for each Elected Member. Even though the onus falls on Elected Members to make these arrangements, failure to comply with the regime and any subsequent sanctions against Elected Members would inevitably cause some reputational concerns for the Council and indeed have them removed from accessing the Council's network.

5.2 Option 2 – Elected Members adhere the Council's compliance regime

This option would be the simplest to adopt as the Council's policies and procedures comply with all relevant Legislation and are updated when required or reviewed by their Information Governance Board on an annual basis, whichever is earlier. The Council's IT Service oversee the annual online mandatory training sessions, support the incident reporting processes and keep abreast of changes to Legislation. As well as providing Elected Members with the necessary information and understanding so that they can avoid a breach of Information Governance obligations, Elected Members would also be able to demonstrate compliance with the training requirements to ICO, should the need arise.

5.3 Option 2 is the recommended approach.

6. Implications for local people / service users

6.1 The recommendations within this report would provide the public with the reassurance that the Council and their Elected Members are in full control of their personal information, take their responsibilities seriously and in full compliance with Data Protection Legislation.

7. Financial implications

7.1 There are no financial considerations requiring any decision.

8. Employee implications

8.1 Specialist resources are assigned to undertake these tasks across the Council; therefore there are no additional resource requirements to undertake this recommendation.

9. Communications implications

9.1 To manage the expectations of those affected when delivering this change by directing all communication through the Service Director of Governance and Member Support, Organisation & Workforce Improvement team and Cllr Howard, the Cabinet Spokesperson without Portfolio.

10. Consultations

10.1 The Executive Director of Core received a briefing on 21st July 2017 from the Head of IT (Service Management). Communities DMT received the report from the IT Service Director on 24th July 2017. SMT received a briefing on 15th August 2017 by the Service Director of Governance and Member Support and Head of IT (Service Management).

10.2 Cllr Howard, the Cabinet Spokesperson without Portfolio is due to be briefed by the Service Director of Governance and Member Support and Head of IT (Service Management) after 15th August 2017, once SMT have approved the report to proceed through the Cabinet process.

11. The Corporate Plan and the Council's Performance Management Framework

11.1 One Council – Learning Organisation

Elected Members should have access to the appropriate knowledge and tools to meet these demands within their communities.

12. Promoting equality, diversity, and social inclusion

12.1 The equality characteristics have been considered within the information governance policies, procedures and education modules. It is recommended

that face to face training is delivered to Elected Members to ensure that the pace of learning is controlled. The training will be delivered within an accessible venue. To conclude there are no adverse impacts on Elected Members.

13. Tackling the Impact of Poverty

13.1 N/A.

14. Tackling health inequalities

14.1 N/A.

15. Reduction of crime and disorder

15.1 N/A.

16. Risk management issues

16.1 The Strategic Risk Register has information governance and cyber security detailed within; the risk of inadequately protecting personal and sensitive data is ominously high. This risk is contributed significantly by people, and their ability to make genuine mistakes with high consequences.

16.2 When a risk becomes an issue; Elected Members should follow the Council's procedures with regard to containing the incident, reporting to the Information Governance team via the IT Service Desk in a timely manner and supporting an investigating officer during their enquiry.

16.3 The number of information governance security and cyber incidents is rising, which is a major risk to the Council not only financially but reputationally. IT Services will continue to monitor and analyse incidents and trends to identify major risk areas, feeding these into the Council's Information Governance Board.

16.4 Over the last 12 months the Council has embarked on a campaign of raising awareness of information governance and security issues. This has been achieved through targeted simulated phishing campaigns detailed within Appendix B - Phishing Campaign. The awareness campaigns do appear to be working; this is evidenced by the increased number of reporting incidents of phishing and malicious e-mails received by users. Last year saw a 240% increase in the number of information governance incidents reported with the number of security incidents being reported growing considerably each quarter.

16.5 The campaigns highlighted an area of particular weakness; with 31 Elected Members visiting bogus sites and of those 16 entered their network user credentials. The sites were visited a total of 152 times by Elected Members with 54 attempts to insert their user credentials.

17. Health, safety, and emergency resilience issues

17.1 There are no immediate implications arising directly from this report.

18. Compatibility with the European Convention on Human Rights

18.1 The proposal is fully compliant with the European Convention on Human Rights.

19. Conservation of biodiversity

19.1 N/A.

20. Glossary

20.1 N/A.

21. List of appendices

21.1 Appendix A - Examples of ICO Imposed Fines

21.2 Appendix B - Phishing Campaign

22. Background papers

22.1 12 steps to preparing for the GDPR

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Officer Contact:	**Ian Turner** **Service Director (Governance and Member Support)**
Telephone:	**01226 773421**
Officer Contact:	**Sara Hydon** **Head of IT (Service Management)**
Telephone:	**01226 773050**
Date:	**08/08/2017**

APPENDIX A - EXAMPLES OF ICO IMPOSED FINES

The following are ICO enforcements which have been published within the last year. Whilst these examples are not Elective Member specific; they are areas in which they potentially may fall foul as a data controller if they do not fully understand their responsibilities.

Revealing confidential details to a third party without appropriate consent from the data subject.

Regal Chambers Surgery

Date **11 August 2016**
Type **Monetary penalties**
Sector **Health**

A GP practice that revealed confidential details about a woman and her family to her estranged ex-partner has been fined £40,000 by the Information Commissioner.

Accessing personal data without a business need to do so

Beverley Wooltorton

Date **25 October 2016**
Type **Prosecutions**
Sector **Health**

Former administrative employee Beverley Wooltorton has been prosecuted at Ipswich Magistrates' Court for accessing personal information without a business need to do so, a criminal offence under section 55 of the Data Protection Act 1998. She pleaded guilty to accessing the medical records of people that she knew, including estranged family members, whilst employed by Ipswich Hospital NHS Trust. She was fined £650 and ordered to pay a £30 victim surcharge and £638.60 prosecution costs.

Failure to respond to a subject access request

Davies Brothers (Wales) Limited

Date **23 January 2017**
Type **Enforcement notices**
Sector **General business**

Davies Brothers (Wales) Limited has been ordered to respond to a subject access request after the ICO ruled that it had failed to comply with the requirements of section 7 of the Data Protection Act.

Stolen unencrypted laptop containing sensitive data. In addition, the data controller not having correct processes and procedures for homeworking, encryption and use of mobile devices

Data breach by historical society

Date **11 November 2016**
Type **Monetary penalties**

The ICO has fined a historical society after a laptop containing sensitive personal data was stolen whilst a member of staff was working away from the office. The laptop, which wasn't encrypted, contained the details of people who had donated artefacts to the society. An ICO investigation found the organisation had no policies or procedures around homeworking, encryption and mobile devices which resulted in a breach of data protection law.

Selling Data Subject information to a third party

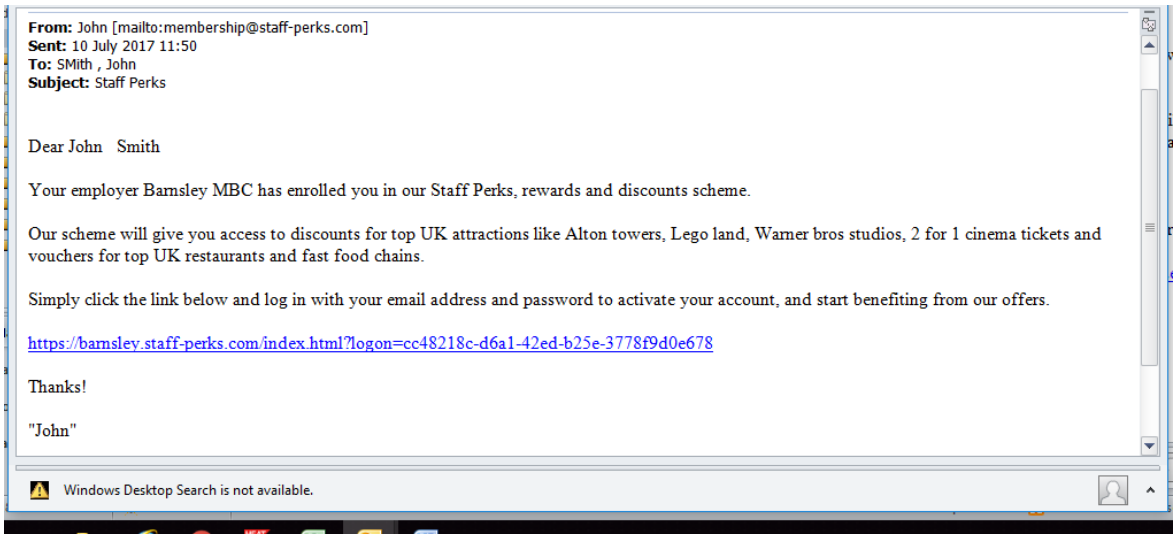
Karun Tandon

Date **02 November 2016**
Type **Prosecutions**
Sector **Finance insurance and credit**

Mr Karun Tandon has been prosecuted at Manchester Magistrates' Court for offences of unlawfully obtaining and selling personal data. The defendant, who worked at Lex Autolease Limited emailed personal data of 551 Lex Autolease customers, relating to road traffic accidents, from his former employer's computer system to his personal email address, which he then sold on to a third party as personal injury leads. Mr Tandon pleaded guilty to two offences under section 55 of the Data Protection Act 1998, and was fined £500, ordered to pay prosecution costs £364 and a £25 victim surcharge.

APPENDIX B - PHISHING CAMPAIGN

Staff Perks phishing campaign:



From: John [mailto:membership@staff-perks.com]
Sent: 10 July 2017 11:50
To: SMith , John
Subject: Staff Perks

Dear John Smith

Your employer Barnsley MBC has enrolled you in our Staff Perks, rewards and discounts scheme.

Our scheme will give you access to discounts for top UK attractions like Alton towers, Lego land, Warner bros studios, 2 for 1 cinema tickets and vouchers for top UK restaurants and fast food chains.

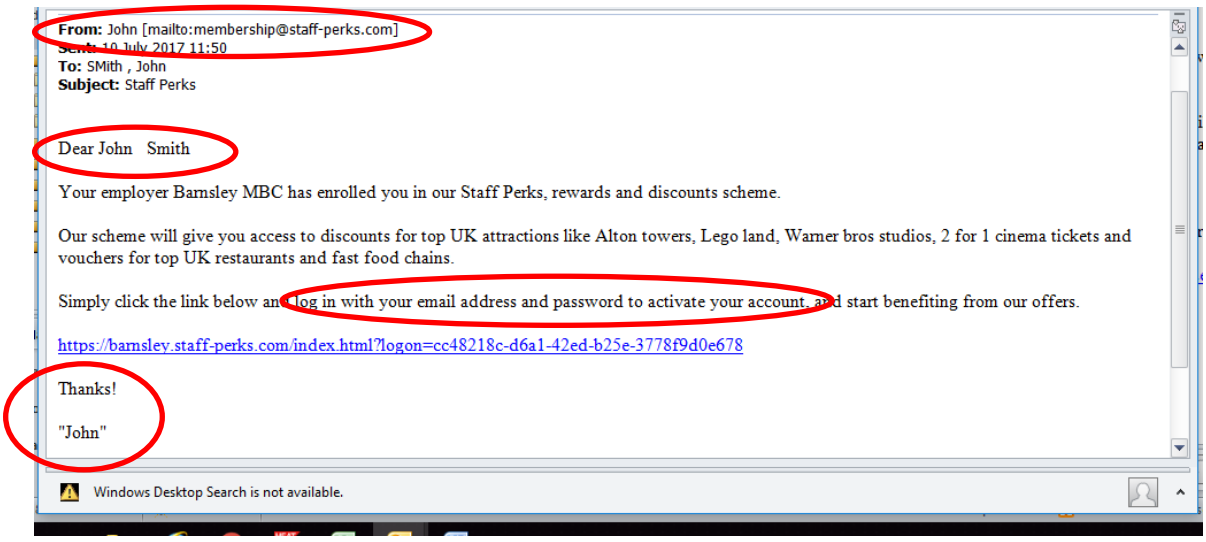
Simply click the link below and log in with your email address and password to activate your account, and start benefiting from our offers.

https://barnsley.staff-perks.com/index.html?logon=cc48218c-d6a1-42ed-b25e-3778f9d0e678

Thanks!

"John"

Windows Desktop Search is not available.



From: John [mailto:membership@staff-perks.com]
Sent: 10 July 2017 11:50
To: SMith , John
Subject: Staff Perks

Dear John Smith

Your employer Barnsley MBC has enrolled you in our Staff Perks, rewards and discounts scheme.

Our scheme will give you access to discounts for top UK attractions like Alton towers, Lego land, Warner bros studios, 2 for 1 cinema tickets and vouchers for top UK restaurants and fast food chains.

Simply click the link below and log in with your email address and password to activate your account, and start benefiting from our offers.

https://barnsley.staff-perks.com/index.html?logon=cc48218c-d6a1-42ed-b25e-3778f9d0e678

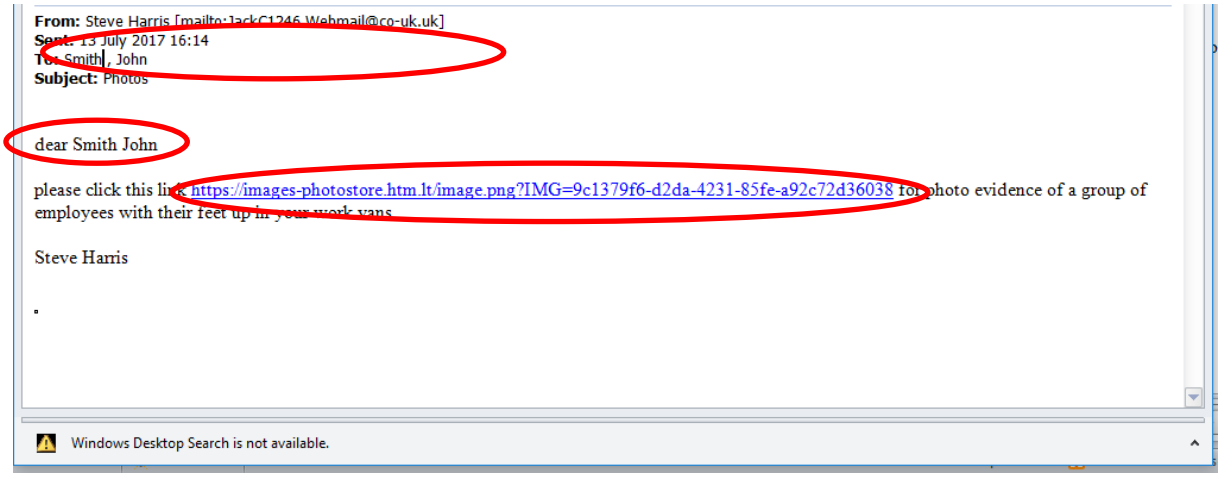
Thanks!

"John"

Windows Desktop Search is not available.

1. From name different to email address
2. Spacing wrong on Dear firstname lastname
3. A legitimate site would send a temp password to login with, not ask for your existing
4. Lack of professional looking signature
5. No prior information from a legitimate internal source advertising Staff Perks, something like this would usually be communicated in straight talk or similar.

Photos phishing campaign:



1. Email address doesn't match the "from" name, also the email domain .webmail@co-uk.uk doesn't look like a common legitimate domain.
2. No capital on dear, first and last name the wrong way around.
3. The domain suffix htm.it on the weblink isn't a commonly used one, you would expect it to be .com or .co.uk
4. There is no mention on the email that this has anything to do with Barnsley Council, and there is very little info. If this was a genuine email from a member of the public you would expect some more information such as a location, or at least a mention of Barnsley.
5. The link goes to a blank page, which prompts a login box asking for your username and password. There is no reason for a website to need your network username and password. If it required a login it would take you to a register page to sign up.