STANDARDS COMMITTEE

Wednesday, 15th February, 2017

at 6.30 pm

Room 102, Hackney Town Hall, Mare Street, London E8 1EA

Committee Membership:

Deputy Mayor Anntoinette Bramble (Chair), Councillor Katie Hanson, Councillor Ben Hayhurst, Councillor Clayeon McKenzie, Councillor Sally Mulready, Councillor Clare Potter and Councillor Jessica Webb (Vice-Chair)

Julia Bennett, George Gross, Adedoja Labinjo and Onagete Louison

Yinka Owa
Director of Legal
Tel: 020 8356 6234
Email: Yinka.Owa@hackney.gov.uk

Contact:
Gareth Sykes
Governance Services
Tel: 0208 356 1567
Email: gareth.sykes@hackney.gov.uk

The press and public are welcome to attend this meeting

Dates of future meetings –

Hackney

AGENDA
Wednesday, 15th February, 2017

ORDER OF BUSINESS

Access and Information

Location

Hackney Town Hall is on Mare Street, bordered by Wilton Way and Reading Lane, almost directly opposite The Ocean.

Trains – Hackney Central Station (London Overground) **–** Turn right on leaving the station, turn right again at the traffic lights into Mare Street, walk 200 metres and look for the Hackney Town Hall, almost next to The Empire immediately after Wilton Way.

Buses 30, 48, 55, 106, 236, 254, 277, 394, D6 and W15.

Facilities

There are public toilets available, with wheelchair access, on the ground floor of the Town Hall. Induction loop facilities are available in the Assembly Halls, rooms 101, 102 & 103 and the Council Chamber. Access for people with mobility difficulties can be obtained through the ramp on the side to the main Town Hall entrance.

Copies of the Agenda

The Hackney website contains a full database of meeting agendas, reports and minutes. Log on at: www.hackney.gov.uk

Paper copies are also available from the Governance Services Officers whose contact details are shown on page 1 of the agenda.

Council & Democracy- www.hackney.gov.uk

The Council & Democracy section of the Hackney Council website contains details about the democratic process at Hackney, including:

- Mayor of Hackney
- Your Councillors
- Cabinet
- Speaker
- MPs, MEPs and GLA
- Committee Reports
- Council Meetings
- Forward Plan
- Register to Vote
- Introduction to the Council
- Council Departments

RIGHTS OF PRESS AND PUBLIC TO REPORT ON MEETINGS

Where a meeting of the Council and its committees are open to the public, the press and public are welcome to report on meetings of the Council and its committees, through any audio, visual or written methods and may use digital and social media providing they do not disturb the conduct of the meeting and providing that the person reporting or providing the commentary is present at the meeting.

Those wishing to film, photograph or audio record a meeting are asked to notify the Council's Monitoring Officer by noon on the day of the meeting, if possible, or any time prior to the start of the meeting or notify the Chair at the start of the meeting.

The Monitoring Officer, or the Chair of the meeting, may designate a set area from which all recording must take place at a meeting.

The Council will endeavour to provide reasonable space and seating to view, hear and record the meeting. If those intending to record a meeting require any other reasonable facilities, notice should be given to the Monitoring Officer in advance of the meeting and will only be provided if practicable to do so.

The Chair shall have discretion to regulate the behaviour of all those present recording a meeting in the interests of the efficient conduct of the meeting. Anyone acting in a disruptive manner may be required by the Chair to cease recording or may be excluded from the meeting. Disruptive behaviour may include: moving from any designated recording area; causing excessive noise; intrusive lighting; interrupting the meeting; or filming members of the public who have asked not to be filmed.

All those visually recording a meeting are requested to only focus on recording councillors, officers and the public who are directly involved in the conduct of the meeting. The Chair of the meeting will ask any members of the public present if they have objections to being visually recorded. Those visually recording a meeting are asked to respect the wishes of those who do not wish to be filmed or photographed. Failure by someone recording a meeting to respect the wishes of those who do not wish to be filmed and photographed may result in the Chair instructing them to cease recording or in their exclusion from the meeting.

If a meeting passes a motion to exclude the press and public then in order to consider confidential or exempt information, all recording must cease and all recording equipment must be removed from the meeting room. The press and public are not permitted to use any means which might enable them to see or hear the proceedings whilst they are excluded from a meeting and confidential or exempt information is under consideration.

Providing oral commentary during a meeting is not permitted.

ADVICE TO MEMBERS ON DECLARING INTERESTS

Hackney Council's Code of Conduct applies to **all** Members of the Council, the Mayor and co-opted Members.

This note is intended to provide general guidance for Members on declaring interests. However, you may need to obtain specific advice on whether you have an interest in a particular matter. If you need advice, you can contact:

- The Corporate Director of Legal, HR and Regulatory Services;
- The Legal Adviser to the committee; or
- Governance Services.

If at all possible, you should try to identify any potential interest you may have before the meeting so that you and the person you ask for advice can fully consider all the circumstances before reaching a conclusion on what action you should take.

1. Do you have a disclosable pecuniary interest in any matter on the agenda or which is being considered at the meeting?

You will have a disclosable pecuniary interest in a matter if it:

i. relates to an interest that you have already registered in Parts A and C of the Register of Pecuniary Interests of you or your spouse/civil partner, or anyone living with you as if they were your spouse/civil partner;

ii. relates to an interest that should be registered in Parts A and C of the Register of Pecuniary Interests of your spouse/civil partner, or anyone living with you as if they were your spouse/civil partner, but you have not yet done so; or

iii. affects your well-being or financial position or that of your spouse/civil partner, or anyone living with you as if they were your spouse/civil partner.

2. If you have a disclosable pecuniary interest in an item on the agenda you must:

i. Declare the existence and nature of the interest (in relation to the relevant agenda item) as soon as it becomes apparent to you (subject to the rules regarding sensitive interests).

ii. You must leave the room when the item in which you have an interest is being discussed. You cannot stay in the meeting room or public gallery whilst discussion of the item takes place and you cannot vote on the matter. In addition, you must not seek to improperly influence the decision.

iii. If you have, however, obtained dispensation from the Monitoring Officer or Standards Committee you may remain in the room and participate in the meeting. If dispensation has been granted it will stipulate the extent of your involvement, such as whether you can only be present to make representations, provide evidence or whether you are able to fully participate and vote on the matter in which you have a pecuniary interest.

3. Do you have any other non-pecuniary interest on any matter on the agenda which is being considered at the meeting?

You will have 'other non-pecuniary interest' in a matter if:

i. It relates to an external body that you have been appointed to as a Member or in another capacity; or

ii. It relates to an organisation or individual which you have actively engaged in supporting.

4. If you have other non-pecuniary interest in an item on the agenda you must:

i. Declare the existence and nature of the interest (in relation to the relevant agenda item) as soon as it becomes apparent to you.

ii. You may remain in the room, participate in any discussion or vote provided that contractual, financial, consent, permission or licence matters are not under consideration relating to the item in which you have an interest.

iii. If you have an interest in a contractual, financial, consent, permission or licence matter under consideration, you must leave the room unless you have obtained a dispensation from the Monitoring Officer or Standards Committee. You cannot stay in the room or public gallery whilst discussion of the item takes place and you cannot vote on the matter. In addition, you must not seek to improperly influence the decision. Where members of the public are allowed to make representations, or to give evidence or answer questions about the matter you may, with the permission of the meeting, speak on a matter then leave the room. Once you have finished making your representation, you must leave the room whilst the matter is being discussed.

iv. If you have been granted dispensation, in accordance with the Council's dispensation procedure you may remain in the room. If dispensation has been granted it will stipulate the extent of your involvement, such as whether you can only be present to make representations, provide evidence or whether you are able to fully participate and vote on the matter in which you have a non pecuniary interest.

Further Information

Advice can be obtained from Yinka Owa, Director of Legal, Tel: 020 8356 6234
Email: Yinka.Owa@hackney.gov.uk

Hackney

MINUTES OF A MEETING OF THE STANDARDS COMMITTEE

THURSDAY, 21ST JULY, 2016

Councillors Present:	**Cllr Katie Hanson, Cllr Ben Hayhurst, Cllr Clayeon McKenzie and Cllr Jessica Webb (Vice-Chair, in the Chair)**
Co-optees Present:	**Julia Bennett, George Gross, Adedoja Labinjo and Onagete Louison**
Apologies:	**Councillor Sally Mulready and Councillor Clare Potter**
Officers in Attendance:	**Patricia Narebor (Head of Commercial) and Robert Walker (Governance Services Officer)**
Also in Attendance:	**Jonathan Stopes-Roe (Independent Person)**

1 Apologies for absence

1.1 As listed above.

1.2 An apology for absence was also received from Yinka Owa, Director of Legal.

2 Declarations of interest

2.1 There were no declarations of interest.

3 Minutes of previous meetings

3.1 **RESOLVED** that the minutes of the:

i) Meeting on 21st January 2016;
ii) Special meeting on 27th January 2016; and the
iii) Extraordinary meeting on 25th May 2016, subject to an amendment to specify that Cllr Webb was elected vice-chair of the Committee;

be approved as true and accurate records.

3.2 The Committee noted the following as matters arising from its recommendations on the Members' Training and Development Programme at its meeting on 21st January 2016 under item 6:

a) Bruce Deville, Head of Governance and Business Development, was now responsible for overseeing the Members' Development Programme;

b) Disability awareness training, and safety and aggression training shall be added to the Member training programme for 2016/17 – dates to be confirmed;

c) Training on Members becoming disabled whilst in office: Bruce Deville would like to clarify the scope of this training but had been unable to contact Cllr Mulready. He will attempt to contact Cllr Mulready again to discuss the recommended training;

d) Risk assessments of Member surgeries had not yet been undertaken. However, Bruce Deville had been in wider discussion with the majority group whip regarding security arrangements for surgeries. Further discussions were due to take place following recess to put support and security measures in place.

3.3 Councillor Ben Hayhurst encouraged the Council to review safety arrangements for Members' surgeries as soon as possible. He also stated that he believed that the Standards Committee should be responsible for reviewing safety arrangements for Member surgeries, if no other committee was doing so, as he believed it was an important area and one which should be overseen by Members.

4 Standards Committee Terms of Reference

4.1 The Standards Committee noted its terms of reference for 2016/17.

5 Standards Committee Draft Annual Report 2015/16

5.1 Patricia Narebor, Head of Commercial (Legal Services), introduced the Standards Committee's Annual Report 2015/16, which was scheduled to be presented to Full Council on 30th November 2016.

5.2 Julia Bennett advised that she had not attended the Standards Assessment Sub-Committee meeting on 25th February 2016, as stated within the Annual Report. The Committee noted that this was an error and that Adedoja Labinjo had in fact attended this meeting.

5.3 **RESOLVED** that the Standards Committee endorses its 2015/16 Annual Report for submission to Full Council, subject to an amendment as identified in paragraph 5.2 above.

6 Standards Committee Draft Work Programme 2016/17

6.1 Patricia Narebor, Head of Commercial (Legal Services), introduced the report on the Committee's draft work programme for 2016/17 and invited comments.

6.2 Julia Bennett queried if a report on whistleblowing could be brought to the next meeting of the Committee. Julia Bennett advised that in the past the Committee had received reports on the Council's whistleblowing policy and she advised that this report had been very useful in helping the Committee to maintain oversight of the Council's ethical framework.

6.3 The Committee also requested an update at its next meeting on safety arrangements for Member surgeries.

6.4 Patricia Narebor agreed to refer the above requests for additional reports to the Director of Legal to confirm if they were within the Committee's terms of reference. Subject to the Director of Legal's agreement, a report on whistleblowing and an update on safety arrangements at Member surgeries would be brought to next meeting.

6.5 **RESOLVED** that the Committee's work programme for 2016/17 be approved subject paragraph 6.4 above.

Duration of the meeting: 6.30 - 6.50 pm

Signed

……..

Chair of Committee

Contact:
Robert Walker, Governance Services

This page is intentionally left blank

Hackney

MEMBERS USE OF ICT | 6TH ANNUAL REPORT	
STANDARDS COMMITTEE **15 FEBRUARY 2017**	**CLASSIFICATION:** **Open**
WARD(S) AFFECTED **All Wards**	
CORPORATE DIRECTOR **Ian Williams, Corporate Director of Finance and Resources**	

1. SUMMARY

1.1. Guidance for Members on the use of Council provided ICT facilities was agreed by Standards Committee on 28th March 2011 following a recommendation from the Internal Audit on Ethical Governance of January 2010 and subsequent questions from new Members during the May 2010 induction process.

1.2. It was also agreed that the Assistant Director – ICT should submit an Annual Report to this Committee on compliance with the Guidance. This is the sixth such report.

2. RECOMMENDATIONS

2.1. Standards Committee is invited to:

- **Note the contents of this report**
- **Comment on the proposed new policy guidance for use of ICT (see section 7)**

3. RELATED DECISIONS

3.1. Revised Draft Guidance for Members on the Use of ICT: March 2011.

3.2. Report of the Internal Auditor on Ethical Standards: January 2010.

4. FINANCIAL CONSIDERATIONS

4.1. There are no direct financial implications arising from this report.

5. COMMENTS OF THE DIRECTOR OF LEGAL

5.1. This guidance is based on the Members' Code of Conduct which provides that Council resources must be used for carrying out Council functions and restrictions are imposed on any significant personal use of such resources. The guidance specifically addresses how Members should use Council provided ICT resources. The Council's policy on using Council systems and data has been refreshed and now clearly applies to Members and their use of Council ICT resources.

6. ANNUAL REPORT 2016

6.1. Previous reports to Standards Committee have referred to municipal years. This has been changed for this report so that it is in aligned with the calendar year, as the report is presented to Standards Committee at the beginning of each calendar year.

6.2. Hackney Council's Member Code of Conduct provides that a Member must act in accordance with the Council's requirements and ensure that Council resources are not used for any unauthorised or political purpose (unless that use reasonably facilitates discharging the Council's functions). This includes Information & Communications Technology (ICT) resources.

6.3. The Guidance for Members on the Use of ICT covers:

- monitoring and compliance
- use of ICT for Council business
- provision of equipment
- using and caring for ICT equipment
- access security and
- general use of ICT, including email, the internet and social media

6.4. The Corporate Director of Finance and Resources first issued the Guidance (via email) to all Members on 1st June 2011. Copies the Guidance were additionally issued to newly elected Members in May 2014.

6.5. Four new Members were elected to office in this reporting period.

6.6. There have been no known or reported breaches of the Guidance during the Municipal year 2015/16 (to date of report publication)

Category	**Number of incidents**	**Description**	**Action taken**
Telephony	0	n/a	
Web / internet	1	Inappropriate content on hard disk.	The Monitoring Officer has taken action in accordance with the Member Code of Conduct.
Email	0	n/a	
Information security	0	n/a	
Total Incidents / Breaches	**1**		

6.7. There have only been three known or reported breaches since the commencement of annual reporting to this Standards Committee in 2013, as summarised in the following table:

Year	Breach category				Description	Data breach	Total
	Telephony	Web / internet	Email	Info security			
2016	0	1	0	0	Inappropriate content	N	1
2015	0	0	0	0	n/a	n/a	0
2014	0	0	0	1	Lost / stolen laptop	N	1
2013	0	0	0	0	n/a	n/a	0
2012	0	0	0	1	Lost / stolen laptop	N	1
Total	**0**	**1**	**0**	**2**			**3**

Note: figures for 2012 - 2015 are taken from the report presented to Standards Committee in January 2016 (http://mginternet.hackney.gov.uk/documents/s47128/Guidance%20for%20Members%20on%20the%20use%20of%20ICT%20-%205th%20Annual%20Report.pdf)

6.8. Monitoring of compliance with the guidance for Members' use of ICT is carried out by Corporate ICT staff reviewing technical logs. Potential breaches may also be notified by Members themselves or by Council staff (for example, Member Services may report a lost phone on behalf of a Member).

6.9. Very exceptionally, a breach might be reported by an external source, such as a member of the public, the Information Commissioner or the police.

6.10. All reported breaches are recorded on the ICT Service Desk system (LANDesk) and passed to the ICT Security Manager for investigation.

6.11. The following paragraphs briefly summarise the control and compliance measures in place for each of the categories in the above tables:

6.11.1. Telephony:

- Mobile phones are only issued to Cabinet Members.
- Members' telephone extensions are included in the Council's monthly telephone performance report. This report provides a summary of the number of calls received and time taken to respond to them.
- Detailed information on individual calls is also available: number dialled/received from and duration.

6.11.2. Web/Internet

- The Council deploys internet monitoring tools which are configured to deny access for staff to certain types of website from the Council's internet connection, including pornographic; homophobic; racist; online gaming; terrorist and computer-hacking sites. (Nb. these filters do not apply when Members use their own personal internet connection or connections provided by other third parties.)
- Standard monthly reports are produced which list the most accessed websites and the most active users. These reports are checked by the ICT Security Manager for any "unusual" activity.
- Individual reports detailing all internet activity can be produced by "user" or "location" on request. Any such requests are logged on the ICT Service Desk system.
- Use of corporate mobile data allowances (eg for tablet devices / laptops) is monitored to identify any excessive use. In the event that data consumption exceeds reasonable levels the Member concerned will be contacted by Member Services and given advice on reducing their data consumption. Any continued excessive use will result in the Member's mobile data service being ceased.

6.11.3. Email

- All email to and from @hackney.gov.uk email accounts is automatically archived and is currently retained for approximately 5 years (this is limited by the size of the archive, rather than by a specific time period). Email that has been deleted from an individual mailbox may still be retrieved from the archive.
- Incoming emails are automatically scanned for viruses and "inappropriate" content. Those which are deemed by the software to contain inappropriate content are held in quarantine and may be released by the receiver if they are satisfied that the content would not breach of Hackney policies or guidance.

6.11.4. Information security

- Lost or stolen devices (phones, laptops, tablets and USB sticks) are reported via the ICT Service Desk. Wherever possible, information is wiped remotely from any such devices to minimise the possibility of any information security breach using device management software.

6.12. Members are listed on the London Borough of Hackney Data Protection Act registration as both Data Subjects and under Sources, Disclosures and Recipients. The Council's current Registration is available on the Information Commissioner's Office website at: www.ico.org.uk. The Registration number is Z8010445 and it runs to 26th June 2017.

7. REFRESH OF THE COUNCIL'S GUIDANCE FOR MEMBERS' USE OF ICT

7.1. The Council is currently refreshing its guidance on secure use of ICT systems and information.

7.2. The new *Using Systems and Data Policy* will ensure that the Council's guidance is up to date with current systems and the latest guidance from UK Government, and is also being reviewed to consolidate the number of policy documents and ensure that it is easy to understand for a non-technical audience.

7.3. In addition to ICT security guidance the refreshed policy will include guidance on use of social media and reasonable use of services such as mobile data. Including these areas in the policy will provide Members with a single point of reference.

7.4. The new policy is due to be approved by the Council's Information Governance Group on 23 February 2017, following which it will be launched to Members, staff and other people who use the Council's systems and information. It will be supported by updated guidance on the Council intranet and online training.

7.5. It is proposed to provide briefings to each political group to support Members in applying the new guidance to their Council work. This will also have the added benefit of providing Members with an opportunity to refresh their understanding of the measures they need to take to protect information that they handle in their work and their responsibilities for Data Protection.

7.6. The latest draft of the new *Using Systems and Data Policy* is attached in appendix 1.

8. REVIEW OF MEMBERS' ICT REQUIREMENTS

8.1. In early 2016 work to pilot improved ICT provision for Members took place. This concluded with recommendations to offer Members a choice of upgrades, based on either a laptop or tablet device. (With Members who prefer to use their own equipment continuing to be able to do so.)

8.2. Most Members have now been issued with their new equipment, with six Members remaining outstanding. These Members have been contacted and dates offered to set them up.

8.3. The ICT team have also reviewed the support and advice provided for all users, including Members. To enhance access to the service, the team are now offering regular 'drop in' support sessions which are open to all. These provide an opportunity to raise issues and get advice, and complement the other support channels (which include telephone and online support)

8.4. Further work to review other aspects of the ICT support for Members has been discussed with Cllr Munn and Cllr Bramble (who holds the lead role for the Mayor's review of support for Members). It has been agreed that once the Town Hall renovation works and set up of Member facilities has completed further discussions will take place with each group to identify other opportunities to review the ICT support provided to Members.

Rob Miller, Director of ICT

Report Originating Officer:	Rob Miller	☎ 020 8356 2600
Financial considerations:	Yasin Razaaq	☎ 020 8356 7298
Legal comments:	Yinka Owa	☎ 020 8356 6234

S.100D Local Government Act 1972 (as amended)

List of Appendices

- Appendix 1: Using Systems and Data Policy

Background documents

No documents which require listing have been relied upon in the preparation of this report.

This page is intentionally left blank

Using Systems and Data Policy

Contents

1. Overview / introduction

All users of the Council's ICT services have a duty to protect the systems, information and data that they use. There is an equally important duty to share information appropriately where this is in the interests of service users (eg where sharing information with partners in health or the police will protect the wellbeing of individuals).

This policy explains your responsibilities in relation to use of the Council's systems, information and data, and how you must use them in such a way that the Council can fulfil its obligations to keep sensitive and personal information secure and deliver high quality public services.

We also have to meet legal and regulatory standards for information security, including:

- Data Protection Act
- Computer Misuse Act
- Freedom of Information Act
- Obscene Publications Acts

If we don't protect the information we use or if we fail to comply with legislation, we could face substantial fines and damage public confidence in us. Our access to essential data that is shared with us by government departments, agencies and other partners to deliver our services could also be taken away.

Staff who do not comply with this policy may be subject to disciplinary action under the Council's Code of Conduct (refer to the Council's Disciplinary Policy and Procedure for details of this).

Any misuse or abuse of Council supplied ICT services or equipment by Members is a breach of

the Council's Member Code of Conduct.

Audience

This policy applies to all users of the Council's systems and data, including:

- Members of the Council
- directly employed staff
- temporary workers (including agency workers, contractors and consultants)
- third parties / any other users accessing the Council's ICT resources (including suppliers, partners, staff working in shared service arrangements, work-experience staff, students)

2. Keeping information safe

This policy explains your duties and obligations for keeping sensitive and personal information secure. It also outlines related Council policies and procedures which you need to comply with.

2.1. Why is this important?

We are trusted with handling sensitive and personal information from a range of citizens, staff, partners and suppliers. We all have a responsibility to keep this safe. If we don't, people and services could be put at risk.

The Council's ICT service is responsible for the implementation, maintenance and management of technical security controls defined in separate ICT security policies. However, most data breaches happen when staff misplace information (eg laptops, papers etc), mistakenly share it with the wrong people (eg by email or fax), or don't dispose of it safely.

This means that we all have a vital role to play in keeping information safe.

2.2. Requirements

To keep the Council's information secure when using its systems, information or data, you **must**:

2.2.1. Make sure you understand and comply with this policy and any other policies, guidelines or legislation specified within it when using the Council's systems and data.

2.2.2. This includes the policy and guidance for use of social media and other online posting in section 4.2.3 below.

2.2.3. Comply with the following policies and procedures:

- the Council's Information Classification and Marking Policy - this explains how you must classify and mark information that you have access to
- the Council's procedures for data protection, including reporting information security breaches
- the Council's records management policies and procedures
- all relevant information sharing agreements when handling data that belongs to a third party organisation (eg government departments, police, NHS partners etc)
- other relevant policies which relate to your area of work, such as those relating to

the Regulation of Investigatory Powers Act (RIPA)

2.2.4. Never attempt to circumvent the security arrangements that have been made to protect the Council's information.

2.2.5. Alert your manager if you believe there has been a breach or potential breach of this policy. Members should alert the Member Services team.

2.2.6. Contact the Council's ICT service if you have any questions about this policy or how to comply with it. Members may also ask the Member Services team for advice and guidance.

2.2.7. Make sure any staff you manage or third parties you have responsibility for (ie by sponsoring their access) are:

- aware of and follow this policy
- suitably trained and have any relevant resources made available (eg appropriate equipment, secure disposal facilities etc)
- provided with, and understand, any changes or updates to this policy

2.2.8. Take reasonable care to protect access to the Council systems, information and data that you have access to, including ensuring that you:

- never share your account password or access to your account with other people (including managers, other members of staff, or with family members and friends)
- never use someone else's account to access the Council's systems, information or data

Be aware that the Council will monitor the use of the communications tools and services that it provides to ensure compliance with this policy and other legal or regulatory requirements. This includes a record of the websites you visit (or attempt to visit) which can be provided to your line manager (or Member Services where these records relate to Members) if inappropriate use is suspected.

By using Council facilities you are accepting that your use is monitored. A disclaimer is automatically attached to each outgoing email to let external contacts know about this monitoring.

2.2.9. Where there is a genuine business need to access information in another user's account or device (eg emails or files in the event of someone not being available due to sickness or annual leave, or for an investigation) or to review monitoring information, a written request approved by a Director (for Members this should be the Council Monitoring Officer) should be submitted to ICT. ICT will only process properly authorised requests and will keep a record of these.

3. Use of devices

This policy explains your responsibilities relating to any device that you use for work (eg laptops, mobile phones, tablets, etc). This includes all devices you have been provided with by the

Council (work devices) and also any personal devices that you use for work purposes / Council business.

3.1. Why is this important?

The option to use a range of devices gives you greater flexibility wherever and whenever you need to do your work. However, you are responsible for making sure that any work-related information which you access or store on any device you use is kept secure at all times.

If you don't take the necessary steps to protect work-related information by following this policy, it could put our customers and services at risk.

3.2. Requirements

3.2.1. General principles

For any device which you use to access or store the Council's information (including phones, tablets and cameras), you **must**:

- take reasonable precautions to protect it from unauthorised access, misuse, damage or theft
- make sure devices are locked and protected by a passcode or password when left unattended (if this function is available on the device)
- notify the ICT Service Desk or Out-of-Hours Service immediately if your device is lost or stolen so they can take appropriate steps to protect your account and any information stored on the device - you must not delay doing this as it could lead to sensitive information being lost (Members may also report lost or stolen devices to the Member Services team, who must notify the ICT Service Desk / Out-of-Hours Service immediately)
- report security concerns in line with the Council's security breach procedures if you believe that unauthorised people may have seen or accessed work-related information or data
- be aware of your environment and not access personal or sensitive information where it could be seen by unauthorised people (eg in a café or on public transport)
- use suitable security equipment (eg a 'Kensington Lock' or lockable storage) to secure equipment in areas that are not protected by access controls (eg swipe access)
- never use public printers or public cloud print services, as this could result in printouts of sensitive information being lost

3.2.2. Work (corporate) devices

During work hours, the Council expects you to use its resources to help you with your job and for business purposes. Reasonable personal use of work devices is permitted provided it complies with this policy and any associated policies and standards specified in it.

When using a work-issued device, you **must**:

- make sure you are using the latest operating system and security software - if you don't know how to download or install these, contact the ICT Service Desk
- make sure that your use of internet / mobile data is within reasonable limits (for example, you **must not** use the Council's internet / mobile data services to stream large videos and **must not** use the Council's mobile data services for extended

internet connection from PCs / laptops – also known as 'tethering'). Excessive use will result in costs being recharged and may also result in the service being cut off
- never allow other people, including family members, to use corporate equipment that has been issued to you
- never install software that is not from a trusted source, as this could introduce malware and information security risks to the device - if in doubt, you must contact the ICT Service Desk for advice
- never install software without complying with copyright and/or licensing requirements
- be aware that the Council is not responsible for, and does not support, any personal applications that you install on the device
- be aware that the Council is not responsible for, and does not support, any personal data stored on the device
- be aware that the Council may delete any personal data or applications that you have installed
- return all work-issued ICT equipment to ICT when you stop working for the Council / stop being a Member, or if required to do so for any reason

3.2.3. Personal devices

When using a personal device for work purposes, you **must**:

- be aware that the Council remains the owner of its information, regardless of whether you store, process or transmit it on your personal device
- be aware that the Council is not responsible for, and does not support, any personal devices
- be aware that if your device is lost or stolen, the Council will take reasonable measures to protect any work-related information that may be stored on it
  - If necessary, this includes deleting ('wiping') all data on the device where this is enabled when you connect to the Council's systems. The Council does not accept any liability for any loss that you incur as a result (eg through loss of personal data on the device).
- download available software updates promptly and use suitable anti-virus protection so your device and any information held on it is protected against vulnerabilities
- never use non-standard versions of a device's operating system software (eg you must not 'jailbreak' or 'root' the device)
- use an account that belongs to and is unique to you
- protect your device with a password that complies with the Council's protocols (as explained when setting up your password for the first time):
  - eight characters long and contains numbers as well as letters (PCs and laptops)
  - five characters long (phones and tablets)
- never download sensitive or personal information onto a personal device (this is especially important for any personal information or information marked OFFICIAL - SENSITIVE).
- never use shared or public computers unless they are protected by an individual account that is used to access the computer, with a password that only you have access to.

3.2.4. USB removable media

When using USB removable media, you **must**:

- only use encrypted USB media devices issued by the Council
- do not use a USB device for general storage (they should only be used for a specific purpose and when there is no other alternative available)
- delete your data from the device as soon as it is no longer needed
- never copy or store third party data (eg government data marked OFFICIAL or OFFICIAL - SENSITIVE) on a USB device without getting explicit written consent for this (eg as part of an Information Sharing Agreement)
- never leave removable media unattended in an unsecure location

4. Use of communications tools and services

This policy explains your duties and obligations when using digital tools, services, applications and extensions that are provided by third parties (eg Trello, Doodle, Dropbox etc).

4.1. Why is this important?

The Council allows staff and Members to use a range of communications tools and services to carry out their work, including online services provided by third parties. This means you can use such tools to plan, manage and deliver your work.

While this gives you the flexibility to use different services, you are responsible for making sure that any work-related information you use is kept secure at all times. If you don't take steps to protect work-related information while using such tools, it could put people and services at risk.

4.2. Requirements

4.2.1. General principles

When using any communication tools, services, apps or extensions to access or store the Council's information, you **must**:

- be aware of, and comply with, guidance provided on the intranet for use of specific tools provided by the Council (eg secure email services, *myoffice* etc) and the business processes for your service area
- never attempt to access Council systems or information for which you do not have authorised access, or which you ought not to have access to (eg if you discover you are able to access files that should not be available to you)
- comply with the Information Classification and Marking Policy (which explains how you must classify and mark information that you have access to) and only use tools that are suitable for the classification level of the information you are accessing or handling
- be aware that other organisations may use different information classification and marking schemes, and that you are responsible for making sure information is handled in line with the Council's policies and procedures, including any information sharing agreements that may exist with partners
- be aware that applications or services that are not provided by the Council may have lower levels of data security and privacy assurance - you must only use Council-assured applications and services for sensitive and personal information
- be aware that agreements or contracts entered into electronically (eg by email) are as binding as written documents (it is your responsibility to ensure that the content of communications are correct)

- take reasonable care to ensure that your communications are addressed / directed to the intended recipients (eg making sure that you use the correct email addresses)
- take reasonable steps to make sure that the person you are communicating with is who they say they are and that they are authorised see the information you are sharing
- take reasonable care when communicating with untrusted and / or unknown contacts
- never click links to URLs (web addresses) or open attached documents received from untrusted or unknown sources or contacts
- never send sensitive or personal information to your personal email account, personal cloud storage service (eg Dropbox, Box.com, SugarSync etc), or other services or applications that are not provided by the Council (eg Trello, Doodle etc)
- never distribute information that is offensive or in any way breaches the Employee Code of Conduct or if you are a Member, the Member Code of Conduct
- do not use Council systems for sensitive personal communications such as medical information or communications with a Trade Union representative. Any email may be monitored and there can be no guarantee of privacy
- do not use Council facilities to circulate unsolicited information to colleagues. This includes circulating information on campaigns and activities not related to the work of the Council

4.2.2. Instant messaging, SMS ('text' messages), video chat and telephone

When you use communications services (eg phone, SMS, Google Hangouts, Skype etc), you **must**:

- make sure you can't be overheard if you are discussing information that is sensitive in any way (eg you must never discuss sensitive or personal information in a cafe or on public transport)
- make sure your camera isn't positioned in such a way that it could accidentally film sensitive documents or computer screens on nearby desks
- make sure your microphone isn't positioned so it can pick up sensitive conversations taking place nearby
- check if the conversation is being recorded. If it is, you must treat the recording in the same way as written communication (ie by following the Information Classification and Marking Policy)
- update any appropriate business systems so that there is a record of any points discussed / decisions made where required as part of your business processes

4.2.3. Social media and other online posting

When posting content online (eg comments, status updates, photos, links, videos etc), you **must**:

- never post information or express views that breach the Council's Code of Conduct (or for Members the Member Code of Conduct), are disrespectful to others or could bring the Council into disrepute
- be aware that you are personally responsible for all content that you publish online
- never post sensitive or personal information which may put individuals or the Council at risk
- never share sensitive (including commercially sensitive) information or personal

information on a public forum or other online service, unless it has been assured by the Council as a safe way to share such information
- make sure you have permission to publish content that may be protected by copyright, fair use or financial disclosure laws
- behave appropriately and professionally, with the understanding that you are representing the Council when using your work persona
- understand that your comments may be associated with your role with the Council even when using a personal social media profile
- alert the Council's Communications Team immediately if the media contact you about anything you have posted online, or if other groups / individuals respond to anything you've posted online in a way that may be contentious or have the potential to bring the Council into disrepute
- never appear to speak on behalf of the Council without authorisation from the Councils Communication Team

Additional guidance for Members

- It is recognised that Council Members may wish to use social media / online posting as part of their political roles. Members are personally responsible for any statements made and must always ensure that they comply with the Member Code of Conduct.
- Members must be be aware that anything they post on social media could be taken as being the official position of the Council. In particular Cabinet Members should take particular care when posting on issues over which they have Cabinet responsibility, especially when there is ongoing consultation or key decisions outstanding.

4.2.4. Fax

When sending information by fax, you **must**:

- be aware that the Council does not consider fax to be a secure way to communicate, especially for exchange of personal or sensitive information
  - It does, however, recognise that some partner organisations (eg NHS partners) can require communication by fax as part of their information sharing agreements, and use of a fax machine or fax service is permitted where an exemption has been approved in advance.
- be aware of and comply with any conditions set out in the authorisation of your request for an exemption to use a fax
- take care to dial the right fax number - accidentally dialling an incorrect destination number is a common cause of data breaches and fines from the Information Commissioner's Office
- be aware that faxes can be read by people not authorised to view the information you are sending (eg if the machine prints off your fax in an open office)
  - To limit this risk, take due care to ensure the correct person receives your fax (eg by calling them in advance to let them know you are about to send it and confirming that they have received the fax).

5. Use of the internet

This policy explains your duties and obligations when using internet services provided by the Council or accessing the internet through work-issued devices.

5.1. Why is this important?

Access to the internet is provided to assist you with your work and service delivery, and you have a duty to protect any sensitive or personal information that you access while using it.

If you don't take steps to keep work-related systems, information and data safe by using the internet responsibly and following this policy, it could put people and services at risk.

5.2. Requirements

5.2.1. General principles

During work hours (including when you are carrying out Council business outside of normal officer hours – eg for Council meetings), the Council expects you to use its resources to help you with your job and for its business purposes. Reasonable personal use of the internet is permitted provided it complies with this policy and any associated policies and standards specified in this policy.

When using internet services provided by the Council, or accessing the internet through work-issued devices, you **must**:

- be aware that the Council uses filtering software to automatically block access to some websites which it considers inappropriate or a potential security risk
- contact the ICT Service Desk immediately if you accidentally visit a site which contains material that might be deemed illegal, obscene or offensive so that it can be added to our list of blocked sites
- make sure that your use of internet / mobile data is within reasonable limits (for example, you **must not** use the Council's internet / mobile data services to stream large videos and **must not** use the Council's mobile data services for extended internet connection from PCs / laptops – also known as 'tethering'). Excessive use will result in costs being recharged and may also result in the service being cut off
- other than for legitimate work reasons (such as managing a complaint from a resident referring to such material), never deliberately view, copy or circulate any material that:
    - is sexually explicit or obscene
    - is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
    - contains images, cartoons or jokes that may cause offence
    - contains material the possession of which would constitute a criminal offence
    - promotes any form of criminal activity
- be aware that if you use the Council's internet services for personal use (eg for online shopping), the Council will not accept liability for default of payment, failure to provide services, or for the security of any personal information you provide online

6. Keeping your working environment secure

This policy explains your duties and obligations for helping to keep your workspace safe and secure.

6.1. Why is this important?

It is essential to be aware of your surroundings and any potential security risks to our systems, information or data. This way, you can take steps to prevent or minimise them. If you don't (or you

simply rely on other people to do this) it could put people and services at risk.

6.2. Your responsibilities

6.2.1. Security badges

When working on site or representing the Council in an official capacity, you **must**:

- keep your security badge (sometimes referred to as a building pass, building access card or ID card) on you and visible at all times. At other times, you must store it in a safe place
- contact the Facilities Helpdesk immediately if your security badge is lost or stolen
- return your badge to your manager when you stop working for the Council (Members must return their badge to Member Services when they stop being a Member)

6.2.2. Visitors and guests

When visitors or guests meet you at an official building or site, you **must** make sure they:

- report to the visitors' reception
- are escorted by a member of staff all times
- wear a visitor's badge at all times and return it when they leave

6.2.3. Buildings and premises

When working at an official building or site, you **must**:

- where it is safe to do so, challenge anyone on the premises who does not have a security badge on display, and if you are not confident that this is safe then you must alert security staff
- alert security staff immediately if you see anyone doing anything suspicious on the Council's premises
- alert security staff immediately if you meet anyone on the Council's premises who can't show you their security badge
- make sure other people don't follow (or 'tailgate') you into secured areas if they don't have an appropriate security badge or access card
- make sure that any storage areas are kept locked and only accessible by authorised individuals

6.2.4. Documents and paperwork

When working with documents or other papers containing sensitive or personal information, you **must**:

- never leave papers unattended, especially in areas where they could be seen by unauthorised people
- keep papers in locked storage (eg a locker or cabinet) when not in use
- take reasonable measures to keep papers secure if you take them away from the Council's premises
- dispose of papers containing sensitive or personal information securely by using a secure waste bin or shredder
- return to the Council any information held on paper or non-corporate services /

systems when you leave

- never write down or print off any passwords or codes that allow access to systems or services that use or store work-related information (if you need to keep a record of your passwords, you must use a password-protected document or an approved password storage application)
- report security concerns in line with the Council's security breach procedures if you believe that unauthorised people may have seen or accessed work-related information or data

7. Version history

Version ref	Author	Comments	Approved by Information Governance Group
0.1	Rob Miller	Original draft	22 October 2016
1.0	Rob Miller	Final draft for IGG approval	23 February 2017

This page is intentionally left blank

Hackney

REVIEW OF THE REGISTER OF MEMBERS' AND CO-OPTEES' DECLARATION OF INTEREST FORM

STANDARDS COMMITTEE **15 February 2017**	**CLASSIFICATION:** **Open**
WARD(S) AFFECTED **All Wards**	
CORPORATE DIRECTOR **TIM SHIELDS - CHIEF EXECUTIVE**	

1. SUMMARY

1.1 The Localism Act 2011 requires all local authorities to adopt a Code of Conduct for its elected Members and voting co-optees.

1.2 The Relevant Authorities (Disclosable Pecuniary Interests) Regulations 2012 requires all Members to complete a declaration of interests form on their election to office, and for voting co-optees to complete a form on their appointment to office.

2. RECOMMENDATION

2.1 The Standards Committee is asked to note the report.

3. REASONS FOR THE DECISION

3.1 This report is for noting and an annual review of the forms, will continue to help develop the arrangements for managing Members' declarations of interests.

4. COMMENTS OF THE GROUP DIRECTOR OF FINANCE AND RESOURCES

4.1 There are no financial implications arising out of this report.

5. COMMENTS OF THE DIRECTOR OF LEGAL, HR AND REGULATORY SERVICES

5.1 The Relevant Authorities (Disclosable Pecuniary Interests) Regulations 2012 provides that Members and co-optees must complete a declaration of interest form.

5.2 The Council's Code of Conduct has implemented the Regulations and provides that all Members and co-optees (including non-voting co-optees) must complete a declaration of interest form.

5.3 Standards Committee further requires regular review of compliance with the Regulations and the Code of Conduct by the Monitoring Officer.

6. BACKGROUND

6.1 The Localism Act 2011 places an obligation on all local authorities to promote high ethical standards in public office.

6.2 Regulations also require Members and co-optees to be transparent and declare all disclosable interests on their declaration of interest form.

6.3 The declaration of interests forms are held in a hard copy register and on the Council's website as well.

6.4 Having reviewed the forms, the majority of Members have been keeping their forms updated. For the small minority who have not submitted a form recently, they have been invited to review their forms to see if any further updates are necessary. By law Members must notify the Monitoring Officer within 28 days of a change in circumstance.

6.5 Appropriate advice and guidance is sent to Members as and when necessary, to keep them updated on case law relating to declarations of interest

Report Author	Tess Merrett Governance Services Manager
Comments of Finance and Resources	Jackie Moylan, Director of Finance jackie.moylan@hackney.gov.uk 020 8356 3032
Comments of Legal HR and Regulatory	Yinka Owa, Director of Legal yinka.owa@hackney.gov.uk 020 8356 6234

This page is intentionally left blank

Hackney

UPDATE ON MEMBERS' TRAINING AND DEVELOPMENT PROGRAMME

STANDARDS COMMITTEE **15 February 2017**	**CLASSIFICATION:** **OPEN**
WARD(S) AFFECTED **ALL WARDS**	
GROUP DIRECTOR **TIM SHIELDS - CHIEF EXECUTIVE**	

1. INTRODUCTION

1. This report provides an update with regards to the Members' Training & Development Programme the aim of which is to provide the necessary training and tools to members to enable them to reach their full potential in their various roles as councillors.

2. RECOMMENDATION

2.1 Standards Committee is recommended to note the update with regards to the Council's member training and development programme.

3. REASONS FOR THE DECISION

3.1 To note.

4. COMMENTS OF THE GROUP DIRECTOR OF FINANCE AND CORPORATE RESOURCES

4.1 The report seeks the Standards Committee to note the update with regards to the Council's member training and development programme.

4.2 The financial impact of the report is minimal as any cost arising will be funded from existing local budgets.

5. COMMENTS OF THE DIRECTOR OF LEGAL SERVICES

5.1 Standards Committee is responsible for monitoring the Council's training and development programme for elected Members and voting co-opted Members. The Member Training and Development Programme should be designed to provide appropriate, comprehensive support for Members' training and development requirements to enable them to fully undertake their roles as elected Members and voting co-optees.

6. BACKGROUND

6.1 To address the Mayor Glanville's commitment in September 2016: "We have an amazing group of councillors, but they need to be supported - so I will launch a review of how we support them" - a fresh look at member training was undertaken resulting in a change in focus, launched in early 2017.

7. TRAINING & DEVELOPMENT OFFER

7.1 The training 'offer' focuses on a more individual approach to training to meet individual needs and aspirations and includes:

- Individual Personal Development Plans (PDP) (optional) which will meet each Councillors' area of work (e.g. committee) and their stated interests and personal aspirations. PDPs will also form part of regular discussions between the Mayor and his Cabinet Members.
- Using established training resources from LGA and LGIU with the focus on member individual development. These are tailor courses delivered through varying formats from e-learning to detailed multi courses and peer support. The LGA/LGIU offer is designed specifically for members and has had extensive member input in its design and delivery.
- 'In house' briefing sessions on key subject areas for the borough, including 'hot topics' e.g. the Housing Bill and Social Housing in Hackney
- Ensuring statutory or role enhancing training is delivered (e.g. Planning, Licensing)
- Training and information around resident or personal welfare – e.g. personal safety and mental health first aid.
- Making appropriate officer briefing notes available to all members via a web page
- Access to the Council's 'learning hub' for on line learning courses including seven courses dedicated to members.
- One to one sessions with officers where in depth knowledge or briefing is required.
- External training courses and briefings where required
- 'Back to the floor sessions' offered from services across the council to give members insight and knowledge into individual service delivery and resident demand.
- An induction programme for new Councillors
- Focussed training for Cabinet Members managed through the Mayor's office.

7.2 A dedicated members training web page is being introduced to ensure all the relevant information is easily accessible and in one place. This will include links to all the main components such as LGA/LGIU & learning hub, dates of briefing and back to the floor sessions, PDP templates and guidance, as well as key contacts. It will be the main landing page for all training and development for members and they should be able to find either the information or a link to it.

7.3 New members need particular and focussed support in their role. Induction programmes are run at the start of each term of office with additional one off introductory sessions run. However new councillors also start during administrations following by elections and particular attention needs to be given to these members to ensure they are able to start their role as fully as possible as quickly as possible as the cycle of council meetings normally does not break for by elections. Induction to the council should include the following and be wider than training courses and cover all aspects to help the councillors undertake their role

- Meeting with the Chief Executive to understand the strategy for the council
- Meeting with Member Services to develop a PDP
- Meetings with other key senior officers (as appropriate) to gain deep knowledge in areas of interest and ward issues
- Code of conduct (compulsory)
- Payroll & declarations information (compulsory)
- Training specific to any appointments
- Information and guidance around casework and surgeries including members support
- Information around the working and functions of the Council (officers and members)
- ICT hardware and practical set up including accessing emails and meeting papers, casework on Covalent
- Buddying with another Councillor
- Relevant LGIU or similar courses for new Councillors eg personal safety
- Member information booklet (A new resource being developed to give Hackney specific information that members need all in one place)
- Ward profile information for their ward

7.4 General member training sessions have been arranged in the following areas:

Date	**Session content**
31 Oct 16	Scrutiny Councillors – delivered by Frontline Consulting A questioning and listening skills session that incorporates the following points: □ understanding the role of being a scrutiny member □ working effectively in a group

9 Jan 17	Housing & Planning Act 2016 & related housing matters – delivered by Council Officers
	• Registered Providers RTB/the forced sale of Council homes.
	• Tenancy reform
	• Private rented sector
	• Planning issues
	  ○ Starter Homes
	  ○ Brownfield Land Register
	  ○ Self-Build and Custom House Building Register
	  ○ Local Plans and Secretary of States default powers, and default powers of the Mayor of London
	• Homes for London affordable homes programme/Planning SPG

Date	Session content
17 Jan 17	Personal Safety – delivered by Metropolitan Police A session specifically for Members with a focus on safety for those who hold political office including: 1) Overall threat level to the UK and its relevance to political groups and public workers. 2) Counter Terrorism awareness and better protective security. 3) Stay Safe 4) Q's and A's.
30/31 Jan 17	Recycling Workshops – delivered by Council officers & Cllr Demirci Workshop looking at work being undertaken to improve the Council's recycling performance, including a detailed look at current data and service, future service options and the impact of impending NLWA decisions.
8 Feb 17	Housing Advice – delivered by Council Officers Current rental market situation in Hackney What is driving the market The withdrawal of financial support for households The impact on Hackney Residents Alternative options
Feb/Mar 17 (3 dates)	Mental Health First Aid – A certified MHFA session where members will be able to:: Define mental health and some common mental health issues Identify stigma and discrimination surrounding mental health issues, specifically in relation to young black men Relate to people's experiences and support people in distress, particularly in surgery and lone-worker settings Look after their own mental health.
Mar/Apr 17 (date to be confirmed)	Safeguarding Children – delivered by Council Officers Session to support Members in understanding their role in safeguarding children and what to do if they have concerns. Also to support Members in understanding how Children's Social Care works in Hackney
Mar/Apr 17 (dates to be confirmed)	Making the most of ICT – delivered by Council officers Drop in clinics to help Members get the most from their ICT equipment, focusing on smart working and utilising the App and software installed; including the mod.gov app for Council papers, Outlook, Office and more.
Apr/May 17 (dates to be confirmed)	Casework clinics – delivered by Council Officers Drop in clinics for members to seek advice on and best practice when dealing with casework.

7.5 A new programme of 'back to the floor' style insight and knowledge sessions is being offered to members. These sessions will allow for member to spend a period of time with front line staff undertaking their roles. They allow for greater understanding of services offered and delivered as well as the

demands on services from residents. It also allows for services to learn more about members and how they can better serve them.

7.6 Members will also be invited to 'previews' of new facilities and services to ensure they are fully informed and have sufficient knowledge of them before they are launched to residents.

Report Author	Bruce Devile, Head of Governance and Business Intelligence Bruce.devile@hackney.gov.uk 020 8356 3418
Comments of the Group Director of Finance and Corporate Resources	Mizanur Rahman, Financial Advisor – (Projects) Mizanur.rahman@hackney.gov.uk 020 8356 4223
Comments of the Director of Legal Services	Yinka Owa, Director of Legal Yinka.owa@hackney.gov.uk 020 8356 6234

Hackney

MEMBER SAFETY	
STANDARDS COMMITTEE **15 February 2017**	**CLASSIFICATION:** **OPEN**
WARD(S) AFFECTED **ALL WARDS**	
CORPORATE DIRECTOR **TIM SHIELDS - CHIEF EXECUTIVE**	

1. INTRODUCTION

1. This report provides an update with regards to Member safety, with particular regard to personal safety at ward surgeries.

2. RECOMMENDATION

2.1 Standards Committee is recommended to note the update with regards to member safety.

3. REASONS FOR THE DECISION

3.1 To note.

4. COMMENTS OF THE CORPORATE DIRECTOR OF FINANCE AND CORPORATE RESOURCES

4.1 The report provides an update with regards to member safety.

4.2 The financial impact of this report is minimal and the future costs of safety measures such as ad hoc security identified within paragraph 6.5 will be contained within the existing budget.

5. COMMENTS OF THE DIRECTOR OF LEGAL SERVICES

5.1 The Council has a duty of care to take such steps as is reasonable to keep Members safe when they carry out their functions as elected councillors. Such steps should include provision of information and support as appropriate to enable Members to keep safe in their role as councillors. This report sets out the steps the Council has taken to discharge this duty.

6. BACKGROUND

6.1 Following the tragic death of Jo Cox MP all members were circulated updated personal safety guidance issued by LGIU.

6.2 Officers in Member Services contacted their peers in other authorities to check whether any best or new practise was in place. No new or better practice was found. All members were contacted in early September 2016 to state this, but also to ask them to raise any specific individual concerns so these could be addressed. The feedback to this was limited, with the main concerns being around the venues and lone working.

6.3 Individual support has been given to members to address any specific concerns or threats to safety and this has been supported by Hackney police. This approach will continue.

6.4 To understand and help a programme to address any concerns about venue safety for members' surgeries, a programme of risk assessments will commence in early 2017. These will start with the venues where lone working takes place first.

6.5 If issues are identified from the risk assessments, the Members Services team will work with the members concerned to put in place as many measures as possible to negate these (e.g. pay for ad hoc security). If needs be alternative

venues will be sought. Surgeries however are run at venues with zero cost to the Council, so any new venues would need not to incur cost. There will also be a challenge to keep surgeries within the ward wherever possible to ensure they are local to the residents members represent.

6.6 A training session for all members was run by the Police on 17 January 2017 around safety at surgeries and terrorism threats with particular regard to those in public office. It also afforded all members the opportunity to seek advice and ask questions from the police expert in this area in the borough.

6.7 Further resources on member safety are available from the LGA (including Health & Safety and Resolution & Conflict Management) and LGIU training (Personal Safety for Councillors) resources for members, which are delivered through a mixture of distance learning and training courses. All members have been made aware of the LGA/LGIU resource as part of a refresh of the member training offer.

6.8 Personal attack alarms have been purchased and offered to all members.

6.9 Officers will continue to work to address any concerns that members bring to them around safety.

Report Author	Bruce Devile, Head of Governance & Business Intelligence bruce.devile@hackney.gov.uk 020 8356 3418
Comments of the Corporate Director of Finance and Corporate Resources	Jackie Moylan, Director of Finance jackie.moylan@hackney.gov.uk 020 8356 3032
Comments of the Director of Legal Services	Yinka Owa, Director of Legal yinka.owa@hackney.gov.uk 020 8356 6234

This page is intentionally left blank