Leeds CITY COUNCIL

Report author: Zöe Cooke
Tel: 07891 279607

Report of Director of Resources and Housing
Report to Member Management Committee

Date: 29th June 2018

Subject: GDPR – Members acting as Data Controllers in their own right

Are specific electoral wards affected? If yes, name(s) of ward(s):	☐ Yes ☒ No
Are there implications for equality and diversity and cohesion and integration?	☐ Yes ☒ No
Is the decision eligible for call-in?	☐ Yes ☒ No
Does the report contain confidential or exempt information? If relevant, access to information procedure rule number: Appendix number:	☐ Yes ☒ No

Summary of main issues

1. The General Data Protection Regulation ("the GDPR") became enforceable in all EU member states on the 25th May 2018. The Data Protection Act 2018 ("the DPA 2018"), which replaces the Data Protection Act 1998 ("the DPA 1998"), supplements the GDPR and the main provisions also came into force on the 25th May 2018. These two pieces of legislation comprise the new data protection framework which all data controllers must comply with when processing personal data and / or special categories of personal data (previously called sensitive personal data).
2. To support Members with understanding the new framework, and what this means for Members when carrying out their different roles, the data protection guidance note for Members has been updated to address the requirements contained within the GDPR and the DPA 2018. This guidance note, together with a shortened version, was circulated by group support officers to all Members in advance of the new framework taking effect.
3. When Members are carrying out their constituency work, and acting as a representative of the residents within their ward, they will be acting as data controllers in their own right and, as such, the responsibility to comply with the new framework rests with them. To assist Members with this however, the Council has prepared a pack of the key documents which will help them ensure compliance with the new laws. Members can utilise and tailor the resources as they see fit.

4. Failure to comply with the new regulation could expose Members to a maximum fine of up to 20 million euros dependent on the type of infringement, for which they could be personally liable.

Recommendations

That the Member Management Committee endorse the suite of documents that have been prepared to assist Members.

1. Purpose of this report

1.1 To seek support from Committee members to endorse the GDPR suite of documents produced by the Council to aid Members with compliance with the new data protection framework when acting as data controllers, and to provide the relevant context.

2. Background information

2.1 The new data protection framework builds on the principles contained within the 1998 Act with a greater emphasis on fairness, transparency and accountability.

2.2 The Council has been implementing the new data protection framework under the governance of the GDPR Strategic Implementation Board which oversees the 9 technical work streams set up to ensure that the compliance requirements are scoped out and implemented across the Council. The Council's GDPR Implementation Team and Information Management and Governance (IM&G) Hubs have been working with the 58 GDPR Service Leads appointed across the authority to raise awareness of the new requirements and to ensure that the necessary changes take effect.

2.3 Under the GDPR, a 'data controller' is a person or organisation who, either alone of jointly with others, determines the purposes and means of processing personal data i.e. the 'why' and the 'how'. When Members are undertaking work for the Council, such as committee work or sitting on a board, then the Council is the data controller and, therefore, responsible for compliance with the GDPR and the DPA 2018. However, when a Member is representing constituents then it is the Member him or herself who is the data controller and, therefore, individually responsible for ensuring the processing of personal data meets the requirements of the new framework.

3. Main issues

3.1 Members, as data controllers, are required to have four key documents in place.

3.2 In order to assist Members, officers have produced the GDPR pack for Members which contains the four following template documents which are attached at Appendix 1:

3.2.1 **Data protection policy** – this essentially sets out how Members intend to comply with the 6 data protection principles contained within Article 5 of the GDPR which govern how personal data must be processed. These principles relate to: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality (security). There is a further requirement for data controllers to be able to demonstrate compliance with these 6 principles which is known as the 'accountability requirement'.

3.2.2 **Privacy notice** – the GDPR is more prescriptive about the information to be provided to data subjects than was the case under the DPA 1998 and this is known as the 'right to be informed'. This privacy information is to be provided at the point of collection of personal data from data subjects (the information to be provided differs when personal data has not been obtained from the data subject) and must be concise, transparent, intelligible and easily accessible. Privacy notices should be regularly reviewed to ensure they remain accurate and up to date.

3.2.3 **Record of processing activities** – the requirement to maintain a record of processing activities is a new requirement although it builds upon the information contained within the register entries which data controllers were previously required to notify the Information Commissioner's Office (ICO) of under the DPA 1998. The record of processing is akin to a policy statement in that it sets out, amongst other things, the types of personal data collected, who this is collected from, and who it is shared with.

3.2.4 **Appropriate policy document** – the DPA 2018 introduces additional conditions and safeguards to be met when special categories of personal data (previously called sensitive personal data) is being processed. The majority of the conditions for processing contained within the DPA 2018 require data controllers to have an appropriate policy document in place. This document explains the data controller's procedures for complying with the 6 data protection principles referred to above and explains the data controller's policies in relation to erasure and deletion of personal data.

3.3 The IM&G Service will review the suite of template documents and further develop them as necessary particularly when more guidance from the ICO becomes available.

3.4 Data Controllers are required to pay an annual data protection fee to the ICO unless they are considered to be exempt. This fee replaces the registration requirement contained with the DPA 1998 and is predicated on a 3 tier fee system with £40 being the lowest tier and £2,900 the highest. Members, acting as data controllers in their own right, will fall within the lowest tier and the Council will continue to pay the new data protection fee on behalf of Members acting as data controllers as it did with the previous notification fee.

4. Corporate considerations

4.1 Consultation and engagement

4.1.1 Consultation on GDPR related policies, procedures, guidance / briefing notes and other implementation tools is undertaken via the GDPR Strategic Implementation Board; the Information Management Board, which the former reports into; liaising with key stakeholders, as appropriate, such as DIS, HR, Legal Services; and through pilots with service users within the Directorates.

4.2 Equality and diversity / cohesion and integration

4.2.1 Equality, diversity, cohesion and integration are all being considered as part of delivering the Information Governance and Management Strategy. This refers to the way training is being delivered as well as how policies will impact on staff and partners.

4.3 Council policies and best council plan

4.3.1 A review of all Information Management and Governance related policies is currently underway and a dedicated Policy Review Group has been established. As part of this review the Group will be consulting with internal stakeholders and external peer checking.

4.4 Resources and value for money

4.4.1 To help address the size and complexity of the GDPR work programme, a GDPR Implementation Team was established in August 2017 for a fixed term of 12 months. This team is led by the Information Governance Lead for Access and Compliance and currently consists of two Senior Information Governance Officers from within the IM&G Service. The whole of the IM&G Service are also supporting the programme through providing advice, guidance, and support with completing tasks, to the GDPR Service Leads, fellow officers and senior leadership teams within the Directorates.

4.5 Legal implications, access to information, and call-in

4.5.1 Assurances as to the work undertaken by the Council to comply with the new data protection framework have been provided by the IM&G Service in the last two annual reports to Corporate Governance and Audit Committee and in a separate update report in January of this year which focussed specifically on cyber security and on GDPR.

4.5.2 There are no restrictions on access to information contained within this report.

4.6 Risk management

4.6.1 The new data protection framework provides the ICO with a number of powers in relation to non-compliance by data controllers of the requirements contained therein; these include the issuing of information notices, assessment notices, enforcement notices and penalty notices. In relation to financial penalties, the new framework introduces a two tier fine system with certain infringements resulting in a maximum financial penalty of 20 million euros and others a maximum financial penalty of 10 million euros. This two tier fine system represents a significant increase from the current law which imposes a maximum financial liability on data controllers of £500,000. Where Members are acting as data controllers in their own right, they could be personally liable for such a fine.

4.6.2 Data subjects who have suffered material or non-material damage i.e. financial loss or distress have the right to receive compensation from the data controller for the damage suffered. Again when Members are acting as data controllers in their own right, they could be personally liable to pay such compensation.

5. Conclusions

5.1 Members, when acting in their constituency role, are individually responsible for compliance with the new data protection framework. To assist Members with fulfilling these requirements, a comprehensive guidance note on the GDPR and DPA 2018 has been produced which sets out the data protection implications for when Members are carrying out their different roles. Further assistance has been provided, for when Members are acting as data controllers in their own right, in the form of a GDPR pack which contains four key documents which Members can utilise to aid with compliance.

6. Recommendations

6.1 Member Management Committee is asked to endorse the suite of documents contained within the GDPR pack that have been prepared to assist Members. These documents can be modified as Members deem fit to meet their own requirements.

7. Background documents[1]

7.1 None.

[1] The background documents listed in this section are available to download from the Council's website, unless they contain confidential or exempt information. The list of background documents does not include published works.

Appendix 1

Members' Data Protection Policy Statement

Elected Members

Elected Members need to process personal data and private information (collectively called "data") in order to fulfil their role as elected representatives. If a Member processes data when they're performing a "corporate" role, for example as an Executive Member or as a member of a committee, the Council itself is the data controller, and processing needs to be carried out under the Council's policies and procedures. However, where a Member processes data as part of representing the residents of their Ward, the Member's the controller and therefore needs to have a policy in place to demonstrate how they'll comply with the data protection rules. When they're a controller, a Member's main objective is to use data carefully and proportionately where they need to, to fulfil their constituency role, having regard to individuals' privacy.

As an elected Member, when I'm a data controller I'll strive to:

1. Adopt the least intrusive approach, only collecting and using data when I need to.

2. Always collect, use, store and process all data fairly and lawfully.

3. Make sure my processing of data has a proper legal basis. For ordinary data, consent from individuals usually isn't needed. If I'm acting in the public interest or in the exercise of my official role as a Member, I'll have a proper legal basis. For special category data, (formerly called sensitive personal data) such as data about someone's health, the legal basis will usually be that it's necessary for me to respond to a request from an individual constituent, or it might be necessary for certain other statutory functions or for substantial public interest reasons. I will make sure that where relevant, I follow the appropriate policy document for Members.

4. Make sure I collect data fairly and transparently, and that I provide the right information to individuals I get data from in the appropriate way. Usually, I will be able to rely on the privacy notice for Members which is displayed on the Council's website, and also where I meet my constituents.

5. Always use data in a way which is compatible with the purposes set out in the information I give individuals at the point of collection, or in the privacy notice for Members, or before further processing, or for other purposes which are legally permitted.

6. Only disclose or share data where this is legally permitted, or where I am required to do so by law. If I disclose or share data, I will only do this when I have balanced fairly the individual's privacy rights against the wider public interest. In particular, I will be careful not to disclose anyone's data inappropriately when I use social media.

7. Collect and process only the minimum relevant amount of data which is needed to meet the purpose for which I collected it.

8. Take every reasonable step to ensure that data are accurate and where necessary kept up to date, and make sure that inaccurate data are deleted or corrected without delay.

9. Make sure I don't keep data in a form which allows people to be identified for any longer than necessary, and that I don't keep data at all once the purpose for my processing is complete. Generally, for constituency matters I'll review whether I still need to keep people's special category data after I've held it for 12 months, and no data will be kept longer than my term of office, unless it's necessary for me to pass this on to my successor or to one of the other Ward Members. I'll make sure that all data will be securely destroyed, and I'll take advice from Council officers about how best to do this.

10. Make sure I process data securely, and protect against unauthorised or unlawful processing, and against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data using appropriate technical and organisational measures. These measures will include as appropriate, the pseudonymisation and encryption of data, making sure systems and services are resilient, and that availability and access to data can be restored appropriately, and making sure there is regular testing and checking of how effective these measures are. Generally, even when I'm the data controller, I'll still process data on the Council's devices, and these are up to the proper standard. If I want to process data on my own device, then I'll ask for advice about this from Council officers.

11. Be responsible and accountable for all matters in this Policy Statement, and complete and keep safe the record of processing activities for Members.

12. Not transfer data to any country outside the EU, for example by using a web-based service where data is stored in another country, unless I've checked with Council officers that that country ensures an adequate level of privacy protection, or that I've provided appropriate safeguards.

13. Help data subjects exercise their rights, including the right of access, the right to rectify or complete data, the right to erasure (right to be forgotten), right to restriction of processing, right to data portability, right to object, and right not to be subject to a decision based solely on automated processing, including by always getting appropriate advice from Council officers about how to deal with any requests.

14. Make sure I use systems, technical or otherwise, which "build in" effectively the data protection principles above and safeguards for data subjects. Generally, I will use Council systems which do this.

15. Make sure that by default I only process data which are necessary for the particular purpose, and by default data is only accessible by those people who need to see it.

16. If I need to use someone to process data on my behalf as a data processor, I'll take advice from Council officers to make sure I use only a data processor who provides sufficient guarantees to implement appropriate technical and organisational measures to meet the requirements of data protection legislation, and ensure the rights of data subjects are protected.

17. Notify personal data breaches to the ICO, and communicate personal data breaches to data subjects as required by data protection legislation. To make sure I do this properly, I'll take advice from Council officers as soon as I think I might have lost data, or disclosed it when I shouldn't have, or when someone else might have got unauthorised access to the data I hold.

Members' Privacy Notice

Who I am.

I'm an elected Member of Leeds City Council. The Information Commissioner's Office (ICO) have got my details as a data controller, in relation to personal data processed by me when I'm representing the residents in my Ward.

I will handle any personal data about you in accordance with the policy statement for elected Members. If you would like more information about this, you can read this here.

What will I use your data for?

I use any personal data about you in my constituency role when I'm representing the residents in my Ward, including dealing with casework for constituents and other members of the public, taking part in local community organisations, crime prevention, organising and taking part in community initiatives and events, dealing with Community Committee business, providing local community leadership, and acting as a consultee on matters affecting my Ward. Sometimes I might need to use your data for one of these purposes, where you originally contacted me about something connected with a corporate role I've got with the Council, but I'll only do this where this is compatible with your original reason for contacting me. A full list of the reasons why I may need to use your personal data is contained in Members' record of processing activities which you can read here.

What's the legal basis for this?

In relation to the legal basis for my processing, for ordinary data I don't usually need to have your consent. If I'm acting in the public interest or in the exercise of my official role as a Member, I have a proper legal basis. For special category data, (formerly called sensitive personal data) such as data about your health, the legal basis will usually be that it's necessary for me to respond to a request from you as an individual constituent, or it might be necessary for certain other statutory functions or for substantial public interest reasons. I will make sure that where relevant, I follow the appropriate policy document for Members.

How will I share your data?

If you ask me to deal with a matter on your behalf, I'll use your data in order to pursue the matter you've raised with me. Depending on what the issues are, this might include me sharing your data with Council officers or a range of other public sector, or other organisations, including housing bodies, healthcare bodies, schools, and the Police, or asking them for data about you. A full list of who I might need to share your data with, and who I might need to get your data from, is contained in the Members' record of processing activities which you can obtain from me.

I intend that only the minimum possible amount of data will be shared, as necessary to assist you.
If you give me data about someone other than yourself, I may need to check the facts with that other person. If you ask me to take action on behalf of your friend or relative, I may need to contact that person to confirm that they're happy for me to act on their behalf.

How can you access your data, correct it, etc.?

If you want a copy of any data that I hold about you, or if you want me to update or correct any of that data, or if you want to ask me to delete any of that data, or object to or restrict what I do with that data, or to make your data portable, or if you have any other queries about the data that I hold about you, please contact me. You don't have to provide me with your data, but obviously if you ask me to deal with a matter on your behalf, I might not be able to deal with this effectively, if you don't give me the data I need.

Members' Privacy Notice

How long will I keep your data?

Generally, for constituency matters I'll review whether I still need to keep your special category data after I've held it for 12 months, and none of your data will be kept longer than my term of office, unless it's necessary for me to pass this on to my successor or to one of the other Ward Members. I'll make sure that all your data is be securely destroyed, and I'll take advice from Council officers about how best to do this.

How can you complain?

You've got a right to complain to the ICO about how I handle your data. This page explains how to do this https://ico.org.uk/make-a-complaint/ or you can ring the ICO on 0303 123 1113.

How can you contact me?

My contact details can be found on this page
http://democracy.leeds.gov.uk/mgCommitteeMailingList.aspx?ID=0

Members' Appropriate Policy Document

Appropriate Policy Document for Members

This is the "appropriate policy document" for elected Members of Leeds City Council. It sets out how I will protect your special category and criminal convictions personal data, when as an elected Member, I'm using your data in my constituency role to represent residents in my Ward.

It meets the requirement at paragraph 1 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

It also meets the requirement at paragraph 5 of Schedule 1 to the Data Protection Act 2018 that an appropriate policy document be in place where the processing of special category personal data is necessary for reasons of substantial public interest. The specific conditions under which data may be processed for reasons of substantial public interest are set out at paragraphs 6 to 28 of Schedule 1 to the Data Protection Act 2018. Depending on the circumstances, there are a number of specific conditions which I might need to rely on.

The specific conditions I'm most likely to rely on are paragraph 6 whereby processing is permitted if it's necessary for the exercise of a function conferred on me, or on another person such as the Council, by an enactment or a rule of law, and where it's also necessary for substantial public interest reasons, and paragraphs 23 and 24 which cover processing by me which is necessary to respond to requests by individuals, and disclosures to me which are necessary for me to respond to requests.

Procedures for securing compliance

Article 5 of the General Data Protection Regulation (GDPR) sets out the data protection principles. These are my procedures for ensuring that I comply with them.

Principle 1

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
I will:

- ensure that personal data is only processed where a lawful basis applies, and where processing is otherwise lawful. When I'm processing data which isn't special category data, If I'm acting in the public interest or in the exercise of my official role as a Member, I'll have a proper legal basis under Article 6 of the GDPR. When I'm processing data which is special category data, I'll make sure that I do this on one or other of the legal bases in Schedule 1 mentioned above.
- only process personal data fairly, and will ensure that data subjects are not misled about the purposes of any processing. In particular, I'll make sure I take account of how people's privacy might be affected by my use of their data. In particular, when I need to share data about someone's health, I'll take particular care not to share any more than the minimum necessary to deal effectively with the particular issue I'm seeking to resolve.
- ensure that data subjects receive full privacy information so that any processing of personal data is transparent, in particular by making sure my privacy notice is accurate and up-to-date.

Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
I will:

- only collect personal data for specified, explicit and legitimate purposes, and I'll tell data subjects what those purposes are in my privacy notice.

- not use personal data for purposes that are incompatible with the purposes for which it was collected. If I do need to use personal data for a new purpose that is compatible, I'll tell the data subject first.

Principle 3

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

I will only collect the minimum personal data that I need for the purpose for which it is collected, and I'll make sure I only collect data which is adequate and relevant.

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

I will ensure that personal data is accurate, and kept up to date where necessary, by referring back to people when I need to. I'll be particularly careful about this when I know that my using data which is out of date, could have a significant impact on the people concerned.

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

If I need to keep personal data, I'll also need to keep it in an identifiable form, so that I can make sure I deal with matters on behalf of constituents and others quickly and effectively.

Generally, for constituency matters I'll review whether I still need to keep your special category data after I've held it for 12 months, and none of your data will be kept longer than my term of office, unless it's necessary for me to pass this on to my successor or to one of the other Ward Members. I'll make sure that all your data is be securely destroyed, and I'll take advice from Council officers about how best to do this.

Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Generally, even when I'm the data controller, I'll still process data on the Council's devices, and these are up to the proper standard. If I want to process data on my own device, then I'll ask for advice about this from Council officers

Accountability Principle

The controller shall be responsible for, and be able to demonstrate compliance with these principles.
I will:

- ensure that I complete and keep up to date, the Members' record of processing activities, and provide this to the Information Commissioner on request.
- ensure that I keep my privacy notice up-to-date and accurate.
- take advice from Council officers if I think that my using data in a particular way could create a high risk for individuals.
- make sure I take account of how individuals' privacy could be affected by my use of their data, particularly in my communications on social media.

My policies as regards retention and erasure of personal data

I will ensure, where special category or criminal convictions personal data is processed, that:

- the Members' record of processing activities includes this, and sets out the envisaged time limits for erasure of the different categories of data.
- where I no longer need special category or criminal convictions personal data for the purpose for which it was collected, I'll delete it securely and take advice from Council officers about how best to do this.
- data subjects receive full privacy information about how their data will be handled, including the period for which their personal data will be stored, in my privacy notice.

How can you contact me?

My contact details can be found on this page
http://democracy.leeds.gov.uk/mgCommitteeMailingList.aspx?ID=0

Members' Record of Processing Activities

Record of Processing Activities

To meet the requirements of Article 30 of the GDPR, Members must hold a record of all processing activities they do as a data controller. Processing refers to everything Members do with data, including collecting, storing, sharing and destroying. To meet these requirements Members need to tick the relevant boxes set out below in relation to their Ward/constituency activities.

Your Details

Your name	Enter your name
Your email address	Enter your email address
Your Ward	Enter your ward

What information is collected

Business activities	☐	Case file information	☐	Criminal proceedings, outcomes and sentences	☐
Education and training	☐	Employment details	☐	Family details	☐
Financial details	☐	Genetic and biometric data	☐	Housing needs	☐
Licenses or permits held	☐	Lifestyle and social circumstances	☐	Offences (including alleged offences)	☐
Personal details (name, address, telephone, email)	☐	Physical or mental health details	☐	Political affiliation	☐
Political opinions	☐	Public health	☐	Racial or ethnic origin	☐
Religious or philosophical beliefs	☐	Sex life or sexual orientation	☐	Student and pupil records	☐
Trade union membership	☐	Tenancy or other property ownership information	☐	Visual images, personal appearance and behaviour	☐
Other (if ticked please detail below)	☐				

Enter details if you selected other.

Members' Record of Processing Activities

Who you collect this information from					
Carers, relatives, guardians and/or representatives	☐	Claimants	☐	Complainants, enquirers or their representatives	☐
Constituents and other members of the public	☐	Council staff including volunteers, agents, temporary and casual workers	☐	License and permit holders	☐
Landlords	☐	Offenders and suspected offenders	☐	Other elected Members, and MP's	☐
People captured by CCTV images	☐	Patients or healthcare users	☐	Professional advisers, consultants & other experts	☐
Recipients of grants or benefits	☐	Representatives of other organisations	☐	Students and pupils	☐
Tenants of Council properties	☐	Traders and others subject to inspection	☐	Witnesses	☐
Other (if ticked please detail below)	☐				
Enter details if you selected other.					

Why you collect this information					
Administration and all activities Members are required to carry out as a data controller	☐	Acting as a consultee in relation to Ward matters	☐	Crime prevention and prosecution of offenders including the use of CCTV	☐
Dealing with casework on behalf of constituents and other members of the public	☐	Dealing with Community Committee business	☐	Local community leadership	☐
Maintaining Member's records	☐	Organising and participating in community initiatives and events	☐	Participating in local community organisations Providing surgeries, street surgeries, and house calls	☐
Pursuing issues pertaining to local government generally		Responding to Members Code of Conduct Complaints			
Other (if ticked please detail below)	☐				
Enter details if you selected other.					

Members' Record of Processing Activities

Who you share this information with

Any country outside of the UK	☐	Central government	☐	Credit reference agencies	☐
Community, voluntary and charitable organisations	☐	Constituents and other members of the public	☐	Courts and tribunals	☐
Current past and prospective employers and examining bodies	☐	Customs and excise	☐	Data processors	☐
Educators and examining bodies	☐	Financial organisations	☐	Healthcare professionals	☐
Healthcare, social and welfare organisations	☐	Housing associations and landlords	☐	International law enforcement agencies and bodies	☐
Law enforcement and prosecuting authorities	☐	Legal representatives	☐	Licensing authorities	☐
Local government	☐	Ombudsman and regulatory authorities	☐	Partner agencies and approved organisations	☐
Police complaints authority	☐	Police forces and non-home office police forces	☐	Political organisations	☐
Press and the media	☐	Prisons	☐	Professional advisers and consultants	☐
Professional bodies	☐	Providers of goods and services	☐	Relatives, guardians, associates or representatives of the person whose personal data you are processing	☐
Regulatory bodies	☐	Religious organisations	☐	Security companies	☐
Service providers	☐	Schools	☐	Students and pupils including their relatives, guardians, carers or representatives	☐
Survey and research organisations	☐	The disclosure and barring service	☐	Trade unions	☐
Other (if ticked please detail below)	☐				

Enter details if you selected other.

Time limits for erasure of different categories of data

- The overall time limit for retaining personal data is the period for which a Member is elected. If a Member is then re-elected for a further term of office, data processed during the previous term should only be retained if this is still necessary and can be justified, for example for dealing with a constituent's on-going problem, or for continuing to participate in a local group or organisation. A Member may also need to transfer data on on-going matters to other Ward Members at the end of their term of office.

- Members will take particular care not to continue to store special category data (previously called sensitive personal data) once the purpose for holding it has been fulfilled, and Members will review all e-mails etc. containing special category data after they've held them for 12 months, to see if they still need to be retained, or whether they should securely destroyed. Members will get advice from Council officers about retaining data, and about how to securely destroy data which is no longer needed.

General description of technical and organisational security measures

- Generally, Members will use Council systems and devices for processing data, even when they are the data controller, and these systems and devices are up to the proper security standard. If a Member wants to use a different system or device, they will take advice from Council officers about this, to make sure there is an appropriate level of security.

- Members will also continue to follow instructions and guidance issued by the Council from time to time about organisational security measures, when they are the data controller.