Data Protection Policy

1. Introduction

1.1 Gosport Borough Council is fully committed to compliance with its statutory responsibilities towards personal data under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

1.2 The Council recognises that the proper treatment of personal information is important to its successful operation and to maintaining confidence between the Council and those with whom it carries out business.

2. Scope

2.1 This policy applies to all personal data held by Gosport Borough Council as data controller (where the Council determines the purposes for which the personal data are to be used), including personal data held electronically as part of a computer file or e-mail, in paper files, on audio or video tape, on CCTV or recorded by any other means.

2.2 This policy applies to all employees, contractors, agency staff, public representatives, business partners, agents, volunteers and employees of partner organisations working for or on behalf of Gosport Borough Council, and any other third parties acting on the Council's behalf.

3. Background

3.1 In order to operate efficiently and provide its statutory and discretionary services, Gosport Borough Council must collect and use information about people with and for whom it works. These may include members of the public, employees (past, current and prospective), clients, customers and suppliers. In addition the Council may also be required to collect, hold and use information about individuals to satisfy requirements of central government.

3.2 This personal information must be dealt with properly regardless of how it is collected, recorded, used and disposed of, whether on paper, in a computer or recorded on other material. The GDPR provides legislative safeguards for this personal data.

4. Personal data

4.1 The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

4.2 This is a wide definition and will include almost anything that the Council holds about people, whether they are the Council's customers, suppliers, employees, Councillors, or any other individuals about whom the Council holds information. Every Unit, Section and team will hold or have access to personal data.

4.3 The GDPR applies to personal data which are recorded as part of a 'relevant filing system', that is, a set of information in which the records are structured either by reference to individuals or by reference to criteria relating to individuals (eg. reference number, address) so that 'specific information relating to a particular individual is readily accessible'. The Council should have little, if any, information about individuals that is not held as part of a relevant filing system.

4.4 Information about companies or businesses is not covered by the GDPR.

5. Guiding Principles

5.1 The GDPR protects personal data from misuse and controls how information about individuals is 'processed' by organisations. 'Processing' is very widely defined in the GDPR and includes almost anything that might be done with or to personal data, including organisation, retrieval, consultation, disclosure or destruction.

5.2 Protection for personal information in the GDPR is based upon six principles that guide how personal information is to be treated. Personal data must be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Adequate, relevant and not excessive;

4. Accurate and up-to-date;

5. Not processed for longer than is necessary and in accordance with the data subject's rights;

6. Kept securely;

5.3 The Council shall comply with these guiding principles in its processing of personal data.

6. ‘Fairly and lawfully processed’

6.1 Ensuring fairness in all processing of personal data is at the heart of compliance with the GDPR. Personal data shall only be processed where the data subject has given their consent or where the processing is otherwise permitted by law.

6.2 In practice fair processing means that:

- There must be a legitimate reason for collecting and processing the personal data;

- Personal data must not be used in ways that have unjustified adverse effects on the individuals concerned;

- The Council must be open and honest about how it intends to use the data, and give individuals appropriate privacy notices when collecting their personal data;

- Personal data must be handled only in ways the data subject would reasonably expect; and

- Personal data must not be used unlawfully.

6.3 Privacy notices (sometimes known as ’fair processing notices’) shall be given in writing or orally when personal information is collected by the Council. The notice shall include:

1. That the information is being collected by or on behalf of Gosport Borough Council

2. The purpose for which the personal data is being collected

3. Any extra information needed in the circumstances to enable personal data to be processed fairly.

6.4 The aim is to be clear and transparent so individuals know exactly what is going to be done with their personal information and for what purposes the data may be used. Section Heads shall be responsible for ensuring that appropriate privacy notices are available for their team in consultation with Legal Services, and shall also be responsible for monitoring the collection of data by their team and ensuring compliance with paragraph 6.3 above.

6.5 Members of staff have access to a wide range of personal information that would not be available to a member of the public. This access must not be abused by looking at or otherwise using personal data for private reasons that are unconnected to their official role.

7. Disclosing Personal Information

7.1 Requests for personal information are commonly made by other individuals or third party organisations. Sometimes this forms part of a request for information under the Freedom of Information Act 2000 (FOIA).

7.2 The starting point is that personal data cannot be released to any other person, whether within your own Section or Unit or another Section/Unit in the Council, or to any other organisation unless to do so would be fair and lawful and would not breach any of the data protection principles, or it falls within the scope of an exemption in the GDPR.

7.3 Under the GDPR disclosing personal data to other organisations may be lawfully carried out provided that at least one of the following conditions has been met:

- the individual has given his or her consent to the processing (staff should check whether the disclosure falls within the scope of the privacy notice given when the data was collected);

- the processing is necessary for the performance of a contract with the individual;

- the processing is required under a legal obligation;

- the processing is necessary to protect the vital interests of the individual;

- the processing is necessary to carry out public functions;

- the processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

7.4 If the data is sensitive personal data (including information about racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sexual life, criminal proceedings or convictions) then there are additional conditions that must be satisfied before data can be released. It will rarely be lawful to release sensitive personal data.

7.5 All requests from third parties for personal data must be carefully checked to ensure that the correct statutory power permitting the disclosure is quoted and, where appropriate, sufficient evidence is provided to show that the disclosure is necessary. A written record of the request and justification provided shall be kept in respect of each

disclosure. Advice should be sought from Legal Services if there is any doubt as to whether or not personal data should be disclosed.

7.6 Common requests for personal information will come from the police, the Department for Work and Pensions, other local authorities, partner agencies and Housing Associations. Where there is a data sharing agreement or protocol already in place, the request shall be checked to ensure that it comes within the scope of that agreement.

7.7 Personal data shall not be given to another individual, even if that person is a partner or close relative, without the data subject's written consent.

7.8 Extra care must be taken when a request for personal information or even a request to simply discuss a personal matter is made over the telephone. The person answering the call must take such steps as are appropriate in the circumstances to verify the identity of the individual, such as confirming a date of birth or unique reference number, before discussing any personal information with them. If in doubt, ask that any request is put in writing or made in person accompanied by appropriate identification.

7.9 Most statutory provisions permit rather than compel disclosure, and usually limit the disclosure to only that which is necessary for the purpose. If in doubt personal information must not be released until a check has been carried out with Legal Services.

8. Disclosure of Personal Information to Councillors or MPs

8.1 The office of Councillor does not convey a 'roving commission' to see any information sought within the Council. A Councillor's 'need to know' is a limited right to see information that is necessary to enable them to carry out their official duties as an elected member.

8.2 Where a Councillor is working on behalf of a member of the public and requests personal information about that person, it shall not be provided to the Councillor unless he or she has the individual's written permission. If there is a question as to whether or not the Councillor is entitled to the personal data, the member of staff should refer the matter to their Section Manager or the Borough Solicitor.

8.4 Likewise Members of Parliament do not have a right to be provided with personal data, even if it relates to one of their constituents, unless they can provide written permission from the individual concerned.

9. Data Sharing

9.1 Routine sharing of personal data between the Council and a third party should be governed by a data sharing agreement. Such agreement shall include at least the following information:

- Parties to the agreement
- Description of the personal data to be shared
- Legal basis for the sharing
- Frequency/method of sharing
- Retention of data
- Identify data controller
- Security measures and what will happen in event of data breach

9.2 All data sharing agreements shall be logged with Legal Services.

10. Sharing Between Council Units

10.1 Gosport Borough Council is one data controller and sharing information between Sections is not, therefore, 'data sharing' for the purposes of the GDPR.

10.2 The transfer of personal data between Council Sections is regarded as using personal information for a secondary purpose.

10.3 Nevertheless the same principles apply as for sharing information with an outside organisation. The processing must be fair and lawful and in accordance with the six data protection principles.

10.4 Where personal information is routinely shared between Council Sections a written record containing the same information as in 9.1 above must be prepared and signed by the Section Manager from the relevant Section(s).

11. Deceased Individuals

11.1 The protection given to personal data under the GDPR is only afforded to living individuals. However requests for personal information about deceased people may still be protected from disclosure under other provisions, such as exemptions under FOIA, so requests must still be considered carefully before information is released.

12. Document Retention

12.1 Personal data must not be kept for longer than necessary. The GDPR does not specify what is 'necessary' so each piece of personal information will need to be considered on its own merits taking into

account the purposes for which it is held and in light of the Corporate Document Retention Scheme.

12.2 Each Section should know what personal data is held, where it is held and why. Destruction dates for the data should be built into electronic and hard copy filing systems.

12.3 Each Section shall keep a deletions log containing a description of the data, the means by which it was stored and the date of and reason for destruction.

13. Data Security

13.1 Personal data must be held securely, regardless of whether it is held electronically, in a hard-copy file, or in any other way. Ensuring the security of personal data is one of the greatest ways in which the Council can deliver compliance with the GDPR and avoid accidental data breach.

13.2 Personal data shall only be stored on portable devices such as laptops and memory sticks to the extent that it is absolutely necessary for the performance of Council duties and only using Council-supplied laptops and removable media. Personal information must not be sent to, stored or in any way processed using private devices or computers, or using personal e-mail accounts. This policy shall be read in conjunction with the Council's Home Working Policy, E-mail Acceptable Use Policy, Internet Acceptable Use Policy and Removable Media Policy.

13.3 Home working is only permitted with the express written permission of the employee's Section Manager in accordance with the Home Working Policy. Only in exceptional circumstances should work requiring access to personal data be undertaken away from the office, and then only with the express written permission of the employee's Section Manager.

13.4 Removal of personal data by a member of staff from Council premises for purposes other than home working shall be permitted only in exceptional circumstances and then with the express written permission of that staff member's Section Manager and only to the extent absolutely necessary for the performance of Council duties. This applies to personal data held electronically, in hard-copy files or recorded in any other way. Where personal data is held electronically this data shall only be accessed using Council-supplied hardware and never using employees' own computers, portable devices or other equipment.

13.5 Personal data shall not be stored outside of Council premises overnight unless in exceptional circumstances and only with express written permission from the staff member's Section Manager.

13.6 Every care shall be taken to protect personal data from theft or loss at all times. Particular care shall be taken when carrying personal data on public transport and storing personal data outside of Council premises. Devices or documents containing personal data should not be left in vehicles when unattended.

14. Data Breaches

14.1 The Information Commissioner's Office has significant powers to punish organisations for data breaches and other poor information management practices. The most serious of these is the power to impose a financial penalty of up to €20,000,000.

14.2 If any breach or suspected breach of the GDPR is identified by a member of staff it shall be reported immediately to the Section Manager who will then report it to The Data Protection Officer and Internal Audit in accordance with the Council's Data Breach Policy.

15. Rights of the Data Subject

15.1 Individuals have a number of rights enshrined in the GDPR regarding their personal data. The Council shall comply with these rights.

15.2 The right of access to personal data

15.2.1 The GDPR allows individuals to find out what information is held about them and see copies of it.

15.2.2 The individual is also entitled to be told that the data controller or someone on the controller's behalf is processing data about him/her, to be given a description of the personal data, the purposes for which the data are being processed and a description of those to whom the data may be disclosed.

15.2.3 The data subject is also entitled to receive information as to the sources of the data and, where decisions are made by "fully automated" means, to receive a statement of the logic involved.

15.2.4 Any request by an individual for their personal information (a "subject access request") shall be referred to the Corporate FOI Coordinator who will make the appropriate arrangements for the request to be dealt with. An application form will be sent to the individual and on return of a completed form and proof of identity the Council then has 30 calendar days within which to retrieve and send the relevant information.

15.2.5 This right does not include the right to see information about other people, so any personal data that relates to/identifies third parties must be deleted (or 'redacted') before sending the information out to the data subject. Where it is not possible to delete the third party data sufficiently so as to protect that third party's identity, the Council is not obliged to comply with the request.

15.2.6 The rights of access extend to personal information contained within all Council e-mail accounts including Councillors' e-mail accounts. If private e-mail accounts are used to carry out Council business, the personal data in those e-mails is still subject to the GDPR and therefore is potentially required to be disclosed by law in response to a subject access request

15.2.7 A request for a housing file or other specific documents should still be dealt with as a subject access request.

15.3 Other rights

15.3.1 Data subjects also have other rights:

- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

16. Notification

16.1 As required under the GDPR the Council maintains its data protection notification with the Information Commissioner's Office (ICO). This sets out the classes of personal data it holds, who provides this data, what is done with it and who are the data subjects. The Council's notification can be checked online on the ICO website www.ico.gov.uk.

16.2 Any changes to the ways in which the Council (but not individual Councillors) holds or processes personal data, or the introduction of any new systems used for processing personal data, shall be notified immediately to the Data Protection Officer in order to keep the notification up-to-date.

17. Complaints

17.1 Any complaints received from data subjects about the use of their personal data shall be referred to the Data Protection Officer and shall not be dealt with under the Council's Corporate Complaints procedure.

18. Responsibility

18.1 This policy shall be the responsibility of the Data Protection Officer and shall be reviewed on an annual basis, to ensure that the scope and content of the policy is still appropriate in the light of legal requirements and the Council's practical experience.

18.2 Random audits and checks will be carried out by Internal Audit to ensure compliance with this Policy and to identify any high-risk areas.

18.3 Non-compliance with or breach of this Policy is a serious matter and will be construed as misconduct. Should it be discovered that this policy has not been complied with, or if an intentional breach of these standards has taken place, the Chief Executive, in consultation with senior management, shall have full authority to take such immediate steps as considered necessary, including disciplinary action. A serious breach of the Policy will be considered gross misconduct.