Data Protection Policy

Owner:	**Corporate Manager of ICT and Information Management**
Document ID:	**ICT-PL-0010**
Version:	**1.3**
Date:	**May 2022**

IT HELPDESK: 01473 265555

Table of Contents

Table of Contents

1. INTRODUCTION

1.1 Purpose

1.1.1. The purpose of this document is to state the Data Protection Policy of Babergh District Council and Mid Suffolk District Council (BMSDC).

1.2. Scope

1.2.1. It is applicable to BMSDC Councillors, the employees of BMSDC, any partners, voluntary groups, third parties and agents who BMSDC employees have authorised to access BMSDC information, including contractors. For the purposes of this Policy all these individuals are referred to as 'user' and they are responsible for taking the appropriate steps, as outlined below whilst working with BMSDC information.

1.3. Linked/Other Useful Policies/Procedures

1.3.1 This policy should be read in conjunction with the:-

- Acceptable Use of ICT Policy;
- Freedom of Information Policy;
- Data Quality Policy;
- E-mail Acceptable Use Policy;
- Protective Marking Policy;
- Records Management and Information Handling Policy;
- Password Management Policy;
- Advice from Information Commissioner's Office.

2. EXECUTIVE SUMMARY

2.1 The joint policy outlines the principles of the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations (UK GDPR) and identifies how the Councils will comply with that Act.

2.2 Designated personnel and their responsibilities are identified.

2.3 Specific details on how personal information will be processed are covered including:-.

2.3.1 Notification to the Information Commissioner

2.3.2 Special Categories of Data (sensitive personal data)

2.3.3 Staff records and monitoring

2.3.4 Use of CCTV

2.3.5 Retention and disposal of personal data

2.3.6 Data subject access requests

2.3.7 Disclosure of data to third parties.

2.3.8 Privacy notices

2.3.9 Data breach

2.3.10 Training and awareness

2.3.11 Security

2.4 Further guidance is available on the Information Commissioner's website at the following link: Information Commissioner's Office

2.5 Procedures on accessing and disclosing personal information to individuals and third parties are included.

2.6 The obligations on the Councils, service areas, individual members of staff and Councillors are explained.

2.7 The process for governance and review of the policy is clarified.

2.8 A list of supporting material which can be used in conjunction with this policy is provided.

3. SCOPE

3.1 In order to operate efficiently, Babergh District Council and Mid Suffolk District Council (the Councils) have to collect and use information about people with whom they work. These may include members of the public, service users, current, past and prospective employees, clients, customers, contractors, suppliers and partner organisations. In addition, the Councils may be required by law to collect and use information in order to comply with the requirements of Central Government.

3.2 Personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

3.3 The Councils regard the lawful and correct treatment of personal information as critical to their successful operations, maintaining confidence between the Councils and those with whom they carry out business. The Councils will ensure that they treat personal information correctly in accordance with the law and any third party processing personal information will be required to meet the Councils' standards and comply with instructions from the Councils regarding personal data.

3.4 The Councils fully endorse and adhere to the principles of data protection as set out in the DPA 2018 and UK GDPR

3.5 This policy applies to all employees, elected Members, contractors, agents, representatives and temporary staff, working for or on behalf of the Councils.

3.6 This policy applies to all personal information created or held by the Councils, in whatever format. This includes but it not limited to paper, electronic, email, microfiche and film.

3.7 Elected Councillors should note that they are also data controllers in their own right and are responsible for ensuring any personal information they hold/use in their office as Councillors is treated in accordance with the DPA 2018 and UK GDPR.

3.8 The GDPR does not apply to requests for information about a person if they are deceased. These requests should be processed in accordance with the Freedom of Information Act (FOIA) 2000 but should also be considered fairly and lawfully.

4. THE PRINCIPLES OF DATA PROTECTION

4.1 The GDPR stipulates that anyone processing personal data must comply with **Six principles** of good practice. These principles are legally enforceable.

4.2 This first principle states that personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency) and in particular, shall not be processed unless:

4.2.1 At least one of the conditions in Article 6 of GDPR is met; and

4.2.2 In the case of special categories of personal data (sensitive), at least one of the conditions in Article 9 of GDPR is also met.

4.3 In practice, this means that Babergh District Council and Mid Suffolk District Council must:

4.3.1 Have legitimate grounds for collecting and using the personal data

4.3.2 Not use the data in ways that have unjustified adverse effects on the individuals concerned

4.3.3 Be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data

4.3.4 Handle people's personal data only in ways they would reasonably expect

4.3.5 Make sure they do not do anything unlawful with the data

4.4 We do this by:

4.4.1 Abiding by the law in all activities

4.4.2 Ensuring data subjects are aware of how their data will be used at the time they provide it and not using it for any purpose incompatible with the original stated purpose

4.4.3 Ensuring the data has been provided by a person who is legally authorised, or require, to provide it

4.4.4 Ensuring that the processing of personal data meets one of the legitimising conditions listed in Article 9 of GDPR

4.4.5 Ensuring that all processing of personal data meets one of the following conditions:

4.4.5.1 The data subject gives consent for one or more specific purposes
4.4.5.2 The processing is necessary to meet contractual obligations entered into by the data subject
4.4.5.3 The processing is necessary to comply with the legal obligations of the controller
4.4.5.4 The processing is necessary to meet the vital interests of the data subject
4.4.5.5 The processing is necessary for tasks in the public interest or exercise of authority vested in the controller
4.4.5.6 The purposes of legitimate interests pursued by the controller

4.5 Further conditions are in place for special categories of personal data, (please see section 8)

4.6 The second principle states that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose (purpose of processing)

4.7 In practice this means that we must:

4.7.1 Be clear ('explicit') from the outset about why they are collecting personal data and what they intend to do with it
4.7.2 Comply with Article 13 of GDPR requirements – including the duty to provide privacy notices to individuals at the point of collecting their personal data
4.7.3 Ensure that if Babergh and Mid Suffolk councils wish to use or disclose the personal data for any purpose that is additional to or different from the original specified purpose, the new use is compatible with the original specified purpose

4.8 We do this by:

4.8.1. At the time data is obtained the data subject will be informed of the purpose for which the data is being collected. Purposes may be specified in a privacy notice given in accordance with Article 13 requirements

4.9 The third principle states that personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed (data minimisation)

4.10 In practice this means:

4.10.1 Data must be the minimum necessary for fulfilling the purpose for which they are processing them

4.10.2 We, Babergh District Council and Mid Suffolk District Council will not collect information we do not need

4.10.3 The data must be adequate for need, The scope and amount of data collected must be adequate to allow the stated aims of the processing to be met and no more.

4.11 We do this by:

4.12 Collecting only the minimum amount of personal data required to fulfil the processing needs, or to comply with legal requirements. Additional unnecessary data will not be collected and data will not be held on the off chance that it might be useful in the future

4.13 This fourth principle states that personal data must be accurate and where necessary, kept up to date (accuracy)

4.14 We do this by:

4.14.1 Taking reasonable steps to ensure the accuracy of any personal data obtained; ensure that the source of any personal data is clear; carefully consider any challenges to the accuracy of the information; consider whether it is necessary to update the information

4.15 This fifth principle states that personal data should be kept in a form which permits identification for no longer than is necessary for the purposes for which the personal data are processed (retention)

4.15.1 In practice this means we will need to:

4.15.2 Review the length of time we may lawfully keep personal data

4.15.3 Consider the legitimacy of purpose or purposes for which the council hold information in deciding whether (and for how long) to retain it

4.15.4 Securely delete information that they are not holding lawfully or legitimately

4.15.5 Update, archive or securely delete information if it goes out of date

4.16 We will do this by:

4.16.1 Only holding personal data as long as it I is necessary for the lawful processing purpose for which it has been provided/obtained

4.16.2 If personal data is collected for a specific project, it shall be disposed of as soon as the project comes to an end

4.16.3 Complying with our record retention guidelines, which can be seen on the Babergh District Council and Mid Suffolk District Council web site at:

Records Retention guidelines

4.17 The last principle states that personal data should be processed in a manner that ensures appropriate security of the personal data (security)

4.18 In practice this means we will need to:

4.18.1 Ensure a level of security appropriate to the nature of the data and harm that might result from a breach of security

4.18.2 Design and organise security to fit the nature of the personal data held and the harm that may result from a security breach

4.18.3 Be ready to respond to any security incident swiftly and effectively

4.18.4 Be sure there is the right physical and technical security, backed up by robust policies and procedures and reliable well trained staff

4.18.5 Be clear about who in the organisation is responsible for organising information security

4.19 We will do this by ensuring we have robust technical and organisational security measures including (amongst others):

4.19.1 Password protection of computer systems

4.19.2 Controlled access to Babergh District Council and Mid Suffolk District Council buildings

4.19.3 Access rights of users appropriate to the needs of their job

4.19.4 Management to ensure that performance with regard to personal data is regularly assessed and evaluated

4.19.5 All staff to have a level of understanding of DPA 2018 and UK GDPR commensurate with their duties

4.19.6 Adequate checks to ensure the suitability of all staff who have access to personal data

4.19.7 Management to ensure that everyone managing and handling data is subject to appropriate line management

4.20 Babergh District Council and Mid Suffolk District Council shall have in place appropriate security arrangements covering both physical and technical safeguards. (See section 15 for further details).

5. RESPONSIBILITIES

5.1 Babergh District Council and Mid Suffolk District Council are data controllers under the GDPR Regulations, the Data Protection Officer is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to the Corporate Manager for the Shared Legal Service.

Directors and Corporate Managers

5.2 Directors and Corporate Managers are responsible for ensuring that business areas have processes and procedures in place that comply with the Data Protection Act 2018 , UK GDPR and this policy, they are responsible for ensuring that data is appropriately protected or that controls are in place to prevent access by unauthorised personnel, and that data cannot be tampered with, lost or damaged. This includes ensuring that all staff are aware of their responsibilities under UK GDPR and trained to discharge those responsibilities.

Local Experts

5.3 Local Experts are key members of each of the councils service teams and promote good practice, they achieve this by advising and supporting their Directorates in ensuring compliance with the Data Protection Act 2018 incorporating GDPR and this policy. In addition, all the councils staff will assist in promoting good data protection practice to ensure Babergh District Council and Mid Suffolk District Council is compliant in these activities, all staff will also highlight to the Information Governance Officer any areas where improvements can be made.

Senior Information Risk Officer

5.4 Babergh District Council and Mid Suffolk District Councils Senior Information Risk Officer (SIRO) with specific responsibility for managing information risks on behalf of the Chief Executive and members of Babergh and Mid Suffolk will be one of the Councils' Directors as designated by the Chief Executive.

Data Protection Officer

5.5 Babergh District Council and Mid Suffolk District Councils Data Protection Officer with specific responsibility to ensure the Babergh District Council and Mid Suffolk District Council are compliant with the DPA 2018 and UK GDPR is the Councils' Monitoring Officer.

Information Governance Officer

5.6 The Information Governance Officer (IGO) will act as a link officer between Babergh District Council and Mid Suffolk District Council services and the Data Protection Officer when there is an issue relating to data protection, the IGO will,

5.6.1. Advise the Data Protection Officer if a data subject access request has been received in any service area and support the service in drawing up its response (simple and complex)
5.6.2. Maintain a data / privacy breach notification procedure and register, and assist the Data Protection Officer in reviewing breaches, why they arose and potential system improvements that may be required
5.6.3. Review the various application forms used within services to ensure they include the reasons why Babergh District Council and Mid Suffolk District Council need to collect and store the personal information requested, and how they will use this information (privacy notices)
5.6.4. Determine the extent to which personal information is shared with others and whom it is shared with (internally and externally)
5.6.5. Conduct a regular review of the types of personal data being processed by services, reporting any changes to the Data Protection Officer and ensuring compliance is maintained, as a result ensure any changes required in the Information Asset Register are effected and updates to the IM Risk Register are made.
5.6.6. Maintain a training and awareness programme for all staff
5.6.7. Support services in undertaking Data Protection Impact Assessments

Staff

5.7. All staff have a responsibility to ensure that they comply fully with DPA 2018 and UK GDPR. It is a criminal offence to knowingly or recklessly obtain or disclose personal data. They should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under Babergh District Council and Mid Suffolk District Councils disciplinary procedures.

Councillors (Members)

5.8. Councillors must comply with this policy when handling personal data on council business and be aware of their responsibilities as individuals under GDPR. Although the Data Controller is liable for any mishandling of personal data, Councillors should be mindful that it can be a criminal offence for which they would be personally liable if they were to process personal data in a manner which they know that they are not authorised by the Data Controller to do. A breach of this policy by a Member is a potential breach of the Code of Conduct.

6. AGENTS, PARTNER ORGANISATIONS AND CONTRACTORS

6.1 If a contractor, partner organisation or agent of the Councils are appointed or engaged to collect, hold, process or deal with personal data on behalf of the Council, or if they will do so as part of the services they provide to the Council, the Corporate Manager at least must ensure that personal data is kept in accordance with the principles of the DPA 2018, UK GDPR and this policy.

6.2 Security and Data Protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the Councils. Available from Procurement or IT.

6.3 A data sharing agreement must be in place prior to any work commencing. The Council promotes information sharing where it is in the best interests of the data subject.

6.4 The Councils have information sharing protocols in place and will comply with the standards established in those protocols.

6.5 When information is shared with other organisations or partners, a formal information sharing agreement must be in place that is signed by all parties. Responsibility for its implementation lies with the Corporate Manager.

6.6 Further advice and guidance is available by contacting:

Information Governance Team

7. NOTIFICATION

7.1 The ICO maintains a public register of data controllers. UK GDPR requires every data controller who is processing personal data to notify and review their notification, on an annual basis.

7.2 It is an offence under GDPR if the notification is not kept up-to date, and also an offence to use personal data in a manner which has not been notified.

7.3 It is the responsibility of all Corporate Managers to advise the Information Governance Officer of any changes to the uses of personal data within their service areas as soon as they occur so that Babergh District Council and Mid Suffolk District Councils notifications can be updated

7.4 Babergh District Council and Mid Suffolk District Councils notification will be reviewed annually and kept up-to-date by the Data Protection Officer

7.5 A copy of Babergh and Mid Suffolk council's current notification can be viewed at the Information Commissioner's website: www.ico.org.uk

8. SPECIAL CATEGORIES OF PERSONAL DATA (SENSITIVE)

8.1. Extra care must be taken when processing special categories of personal data as additional requirements under GDPR must be met to ensure that the processing is legitimate and safe. At least one of the legitimising conditions described under Article 6, and also one of the legitimising conditions (Article 9) shown below, must be met.

8.2. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Paragraph 7.2 shall not apply if one of the following applies

8.2.1. The data subject has given explicit consent
8.2.2. It is necessary to fulfil the obligations of controller and data subject
8.2.3. It is necessary to protect the vital interests of the data subject
8.2.4. Processing is carried out by a foundation or not for profit organisation
8.2.5. The personal data has been made public by the data subject
8.2.6. Establishment, exercise or defence of legal claims
8.2.7. Processing is necessary for reasons of substantial public interest

8.2.8. Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

8.2.9. Reasons of public interest in the area of public health

7.3.10 Archiving purposes in the public interest

8.3. Babergh District Council and Mid Suffolk District Council have an Appropriate Policy Document regarding the use of the conditions above and the advice of the Data Protection Officer or their duly authorised deputy should be sought before the processing or collection of sensitive personal data prior to any new purpose commences.

9. STAFF RECORDS AND THE MONITORING OF STAFF

9.1. Babergh District Council and Mid Suffolk District Council should comply with the ICO's 'Employment Practices Code' in relation to the processing of staff personal data. This Code is intended to help employers comply with the DPA 2018 and to encourage them to adopt good practice. The Code aims to strike a balance between the legitimate expectations of staff that personal data about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own organisations carrying out their legitimate business.

In particular, staff monitoring should only be carried out in accordance with this Code. A copy of the Code is available on the ICO website.

10. ACCESS RIGHTS BY INDIVIDUALS – DATA SUBJECT ACCESS REQUESTS (DSARS)

10.1. An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a DATA Subject Access Request under the GDPR.

10.2. Under normal circumstances no fee is payable for access to records applications, the councils must provide a copy of the information **free of charge**, however, the council can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. The council may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge for all subsequent access requests. This charge would be subject to the view of the Information Governance Officer.

10.3. Under the GDPR Babergh District Council and Mid Suffolk District Council may receive DSAR requests for a number of reasons based upon the rights individuals are granted, these rights are as follows:-

1. **The right to be informed** what Personal Data Babergh District Council and Mid Suffolk District Council collects from individuals , why Babergh District Council and Mid Suffolk District Council collect it and how Babergh District Council and Mid Suffolk District Council will use it, this is communicated to individuals within our Web site section "Your Right to Information" which can be found on the Councils web site at: How we use your information
2. **The right of access,** Babergh District Council and Mid Suffolk District Council are obligated within UK GDPR to allow access to Personal Data so that individuals are aware of and can check it is correct and being processed as allowed by the regulations. The way individuals can gain access to their Personal Data we are holding is by completing and providing a Data Subject Access Request to Babergh District Council and Mid Suffolk District Council
3. **The right to rectification** of any errors or omissions individuals believe there may be in their Personal Data Babergh & Mid Suffolk District Councils hold, this is often after they may have received their Personal Data having made a Data Subject Access Request.
4. **The right to erase (Right to be Forgotten),** there are some specific circumstances where individuals can request the erasure of their Personal Data, these include:
   a) Where the Personal Data is no longer required for which it was originally collected or processed.
   b) When the individual withdraws consent, (unless the Personal Data is collected and or processed as a legal obligation or is required for Babergh District Council and Mid Suffolk District Councils performance of tasks they carry out in the public interest or in the exercise of official authority).
   c) When the individual opposes the Babergh District Council and Mid Suffolk District Council processing their Personal Data and Babergh District Council and Mid Suffolk District Council have no superseding legitimate interest for continuing the process.

d) If Babergh District Council and Mid Suffolk District Council have unlawfully processed the individuals Personal Data.
e) If there is a legal obligation for Babergh District Council and Mid Suffolk District Council to remove the individuals Personal Data.
f) If Personal Data is processed in relation to the offer of information tor society services to a child, one of the specified circumstances in which the right to erasure applies is when you collected the personal data of a child under the lawful basis of consent, when offering an ISS directly to a child. It should generally be as easy for a child to exercise their right to erasure as it was for them to provide their personal data in the first place.

5. **The right to restrict processing,** Babergh District Council and Mid Suffolk District Council may restrict processing of individuals Personal Data for a number of reasons detailed in the points below:

a) While considering and responding to individuals if they have questioned the accuracy of their Personal Data which Babergh District Council and Mid Suffolk District Council are holding and or processing.
b) Where individuals have objected to the processing of their Personal Data and where it is obligatory for the Babergh District Council and Mid Suffolk District Councils performance of a public interest task while BMSDC consider if the Council's legitimate grounds outweigh the individuals objection. If Babergh District Council and Mid Suffolk District Council decide to restrict processing for this reason Babergh District Council and Mid Suffolk District Council will contact the individual when a decision is made to continue processing.
c) If Babergh District Council and Mid Suffolk District Council no longer require the individuals Personal Data and they require their Personal Data to establish, exercise or defend a legal claim.
d) If Babergh District Council and Mid Suffolk District Council processing is found to be unlawful and the individual does not want BMSDC to erase their data but request Babergh District Council and Mid Suffolk District Council to restrict processing instead.

6. **The right to data portability,** this allows individuals to make a request to acquire and reuse their Personal Data for their own purposes across different services. This right does not apply to the data that Babergh District Council and Mid Suffolk District Council has if required for the councils performance of tasks Babergh District Council and Mid Suffolk District Council carry out in the public interest or exercise of the councils official authority.
7. **The right to object**, An individual is free to object to the Council if they feel their Personal Data is being used for reasons other than communicated in this policy.
8. **Rights in relation to automated decision making and profiling** GDPR requires safeguards to be in place to protect individuals against the possibility that a harmful decision is made without human intervention, individuals can exercise the right to object if this is found to be the case.
9. All DSAR requests must be logged in the Data Subject Access request register.
10. It is in the interests of the Babergh & Mid Suffolk District councils to have an open and honest approach with all individuals on which they hold data.

10.4. UK GDPR sets out guidance and a time limit within which a Data Subject Access Request (DSAR) must be answered.

10.5. Any individual requesting access to their personal data is encouraged to complete a request in writing which must be referred to the Data Protection Officer. This gives clarity around the date the request was made and therefore the deadline date and also encourages the individual to think clearly about the data they require. However, under UK GDPR, personal data requests do not have to be made in writing, a verbal request is just as legitimate.

10.6. Guidance regarding DSARs is available on Babergh District Council and Mid Suffolk District Council website at: How we use information which includes access to a DSAR application form which may be printed off and completed.

10.7. The individual making the request must produce a document such as a passport or driving license to confirm his or her identity, not taking to reasonable steps to confirm the requestor's identity could lead to a breach of information to someone not entitled to it.

10.8. Babergh & Mid Suffolk district councils will approach all requests for data in an open and honest way and seek to ensure that the individual gets all the data they require as long as this is permissible within the law.

10.9. There will be some requests where it will not be possible or appropriate to release personal data, for example, when doing so would involve releasing personal data about another individual, or if the data relates to ongoing criminal investigations. Any concerns about releasing data should be discussed with the Data Protection Officer or their duly authorised deputy prior to release of the information.

More information on the procedure for recognising and responding to a DSAR can be found in Babergh & Mid Suffolk District Councils (BMSDC) Policy for Data Subject Access Requests (DSAR) as required by General Data Protection Regulation (GDPR) Document ID: ICT-PL-0018

11. The Right to be informed and Privacy Notices

11.1. The right to be informed encompasses the councils' obligation to provide fair processing information, typically through a privacy notice. It emphasises the need for transparency over how the councils' use personal data.

11.2. The information supplied in the privacy notice is determined by whether or not the personal data was obtained directly or indirectly from the individual.

11.3. The information the councils' supply about the processing of personal data must be:

11.3.1. Concise, transparent and easily accessible
11.3.2. Written in clear and plain language, particularly if addressed to a child
11.3.3. Free of charge

11.4. Further guidance on how to comply with 'the right to be informed' is provided in the: ICO Right to be informed

12. DISCLOSURE OF PERSONAL INFORMATION ABOUT THIRD PARTIES

12.1. Personal data must not be disclosed about a third party, except in accordance with the UK GDPR.

12.2. If you believe it is necessary to disclose information about a third party to a person requesting data, you must seek advice from the Information Governance Officer

12.3. The responsible Corporate Manager must ensure all contractors and individuals working for or on behalf of the Councils within their service areas must be appropriately trained and also ensure identity checks are undertaken before providing any personal data.

12.4. INFORMATION & DATA SHARING

12.5. The Councils may share information when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

12.6. Information must always be shared in a secure and appropriate manner and in accordance with the information type and classification.

12.7. The Councils will be transparent and as open as possible about how and with whom data is shared; with what authority; and with what protections and safeguards.

12.8. Where requests are received from external organisations or third parties for personal data about individuals, advice should be sought from the Data Protection Officer, Information Governance Officer or their duly authorised deputy unless there is an up-to-date information-sharing/data exchange agreement in place with that organisation or third party.

12.9. Agencies which request data on a regular basis such as the police or banks will have easy access to appropriate paperwork and guidance for use in these circumstances. Section 29(3) allows a data controller to disclose personal data to a third party where the disclosure is made for any of the crime prevention or taxation purposes listed in 29(1) if applying specific provisions in the DPA would be likely to prejudice the purposes by preventing the disclosure. For example Suffolk Constabulary provide a form “DECLARATION FORM FOR DATA USER” which will contain details of the request and be signed by the investigating officer and authorised by a senior officer. All requests must be referred to the Information Governance Officer.

12.10. It should be noted that whilst staff understandably will wish to assist external agencies wherever possible especially if the request relates to criminal activity (for example the police or banks), Babergh District Council and Mid Suffolk District Council are under no obligation to release personal data unless the request is made by a court order. No information should be released and all requests referred to the Information Governance Officer.

12.11. Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasions it may be appropriate to publish personal data

with the individual's consent. However, in such cases staff must ensure consent is 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately.

12.12. Staff should be aware that publishing personal data on Babergh and Mid Suffolk councils' web pages or on the internet by any other means effectively means that the data is published world-wide. This means it cannot be protected by UK GDPR. Great care should be taken before publishing any personal data (or any data from which individuals could be identified) in this manner and the approval of Babergh District Council and Mid Suffolk District Councils Data Protection Officer and Senior Information Risk Owner or their deputies should be obtained before publication.

13. WHAT TO DO IN THE EVENT OF A DATA BREACH

13.1. The ICO defines a data breach as a 'breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provisions of a public electronic communications service'.

13.2. A personal data breach includes but is not restricted to the following:

13.2.1. The accidental alteration or deletion of personal data

13.2.2. The transfer of personal data to those who are not entitled to receive it

13.2.3. Unauthorised access to personal data

13.2.4. Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could not have reasonably contemplated

13.2.5. Theft of storage devices

13.3. Babergh District Council and Mid Suffolk District Council must verify and report incidents to the Information Commissioners Office within 72 hours of being identified to comply with the General Data Protection Regulations.

13.4. Depending on the type of incident please report as shown below:

13.4.1. In the event of a data breach

13.4.1.1. Report an Information Security incident on the Information management Connect website at, **Report an Information Management Issue**

13.4.1.2. Inform Line Manager

13.4.2. In the event of a virus or Cyber attack

13.4.2.1. Take a photo or video of the PC screen.

13.4.2.2. Shut the PC down immediately, **DO NOT** USE your PC to raise a report.

13.4.2.3. Phone the IT Help desk and report the problem on **01473 265555**

13.4.2.4. Take the PC to the IT help platform in Endeavour House.

13.4.2.5. Inform Line Manager

13.4.3. In the event of a loss or theft of IT equipment

13.4.3.1. This would include, mobile phones, Personal Computers and memory sticks.

13.4.3.2. Phone the IT Help desk and report the theft/loss on **01473 265555**

13.4.3.3. Using an alternative PC (If available) report an Information Security incident on the Information management Connect website at, **Report an Information Management Issue**

13.4.3.4. Inform Line Manager

13.5. The Data Protection Officer or their duly authorised deputy will then decide on the most appropriate steps to take depending on the nature and quantity of data released. An investigation will be carried out into all data breaches.

13.6. The ICO will be informed of all serious data breaches where significant harm to an individual(s) is likely or a large number of individuals are affected.

13.7. More information on reporting personal data breaches can be found in Babergh and Mid Suffolk District Councils policy, ICT-PL-0019 Reporting Personal Data Breaches.

14. TRAINING AND AWARENESS

14.1. In order to fully comply with GDPR it is important that all staff who have access to any personal data have an awareness of the regulations.

14.2. Training is a crucial element of staff awareness Babergh District Council and Mid Suffolk District Council staff must be aware of their obligations relating to personal data as part their duties.

14.3. Training may be achieved in a number of ways: all staff to be made aware of this Data Protection Policy; e- learning tools; and in-house training provided by the Data Protection Officer or their duly authorised deputy.

14.4. For some posts additional training and guidance is required. Those posts will identified through their work and any additional training and guidance will need to be discussed with the line manager in the first instance.

15. KEEPING INFORMATION SECURE

15.1. The Sixth Principle of GDPR requires organisations to take appropriate technical and organisational measures to keep data secure. The security of data held by Babergh and Mid Suffolk councils is a relatively complex area and more information on the technical details of information security can be found in the Babergh District Council and Mid Suffolk District Council Information Security Policy: Babergh and Mid Suffolk Security Incident Management Policy and Procedure

15.2. However, security of data goes beyond the use of computer equipment. Data will inevitably be stored or processed in hard copy forms at some time and access to this must be restricted to only those authorised to view it. As a general guide hard paper copies should not be left in the open in offices but should be kept locked away when

not in use, in the same way as computer terminals should not be left unlocked and unattended.

15.3. It is important to remember that individuals should only be able to access data which they need to do their job. Personal data should not be left unattended and freely available to anyone in the office.

Working from home

15.4. When working from home

15.4.1. Officers must ensure they only use their encrypted laptops to access personal data electronically. Paper files which include personal information must be kept in secure cases (lockable) at all times when not in use.

15.4.2. Officers must lock the PC screen whenever the PC is left unattended.

15.4.3. Officers must not allow any unauthorised user access to their PC for use of any kind.

15.5. **UNDER NO CIRCUMSTANCES** should hard copy files be left unattended.

16. DATA QUALITY, INTEGRITY AND RETENTION

16.1. If an individual requests that personal data held about them be updated because it is wrong, incomplete or inaccurate, the position should be investigated thoroughly, with reference to the source of information.

16.2. A caution should be marked on the person's file to indicate uncertainty regarding accuracy until the investigation is complete.

16.3. The Council will work with the person to either correct the data and/or allay their concerns.

17. RETENTION AND DISPOSAL OF PERSONAL DATA

17.1. It is the responsibility of the service areas holding personal data to ensure that the data they hold is kept accurate and up-to-date and is not held for any longer than is necessary for the purpose for which it was collected.

When the data is no longer required the service area must dispose of the data safely. Guidance on retention periods for classes of data is set out in the Babergh & Mid Suffolk District Councils' record management guidance which is available on the Babergh & Mid Suffolk District Councils website Records Retention guidelines

18. CCTV MONITORING

18.1. CCTV monitoring must only be carried out in accordance with the ICO's code of practice on CCTV. A copy of this code is available on the ICO website at the following link CCTV Code of Practice

18.2. The covert surveillance activities of the law enforcement community are not covered here because they are governed by the Regulation of Investigatory Powers Act (RIPA) 2000 and Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.

19. COMPLAINTS

19.1. Complaints about responses to data subject access requests are dealt with by an internal review.

19.2. Complaints are to be put in writing and sent to the Information Management team or E mailed to the following address:

Information Management Team

DataProtection@baberghmidsuffolk.gov.uk

20. BREACH OF POLICY

20.1. Any breach of this policy should be investigated in accordance with the mandatory procedures specified in the Information Security Incident Management Policy and Procedure.

20.2. The Council will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation.

20.3. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

21. REVIEW OF THE POLICY

21.1. This policy will be reviewed every two years or when any other significant change impacts upon the policy. Comments on the policy, from both employees and members of the Public, are therefore welcome and can be addressed to:-

Information Governance Officer
Babergh and Mid Suffolk District Councils
Endeavour House
8 Russell Road
Ipswich IP1 2BX

21.2. FURTHER ADVICE

For further advice on this policy, please contact:-

Information Management Team
DataProtection@baberghmidsuffolk.gov.uk

APPENDIX 1

DOCUMENT CONTROL

Changes History

Issue No.	Date	Amended By	Summary of Changes
1.0	January 2010	Chief Information Officer	Version 1.0
2.0	March 2015	Neal Scarff Philip Barbrook Duncan Farley	Review and Updates
1.0	April 2015	Carl Reeder	Convert this document for Babergh and Mid Suffolk use
1.1	November 2015	Carl Reeder	Review and Update
1.2	May 2018	Martyn Jackson	Review and update for GDPR
1.3	May 2022	Andy Hope	Review and Update

Authorisation (Responsible Owner)

Role	Name	Approval Date
Corporate Manager for ICT and Information Management	Carl Reeder	May 2018
Head of Corporate Resources	Katherine Steel	May 2018
Corporate Manager – Internal Audit	John Snell	May 2018
Data Protection Officer	Emily Yule	May 2022

Approval (Accountable Owner)

Role	Name	Approval Date
Senior Information Risk Owner	Katherine Steel	May 2018

Reviewers (Consulted)

Role and Review Responsibilities	Name	Approval Date
Corporate Manager for Internal Audit	John Snell	May 2018
Information Management Specialist (Legal Obligation)	Martyn Jackson	May 2018
SCC Policy and Compliance Officer		

BMSDC Information Governance Board	**Arthur Charvonia**	**May 2018**

Distribution List – Once authorised (Informed)

Name	Organisation
All Users	**See Section 1.2.1 of the Policy**

Review Period

Date Document to be Reviewed	By whom
May 2019	**Corporate Manager for ICT and Information Management**
May 2024	**Information Governance Officer**

APPENDIX 2

RESPONSIBILITIES

Babergh District Council and Mid Suffolk District Council

Training – BMSDC will train users with regard to this policy.

Training for Councillors *will be provided as part of the Councillors' Support Programme*.

ICT and Information Management Team

Implementation of Policy – The ICT and Information Management Team has been tasked to implement this policy.

Internal Audit Team

Monitoring of Policy – The Internal Audit Team has been tasked to monitor its effectiveness.

Corporate Managers

Induction, Training and Support – Corporate Managers are responsible for ensuring that adequate induction and training is undertaken by staff and that support is provided to them so as to implement this policy (see 2.4.1).

The Corporate Manager - Governance is responsible for ensuring that adequate induction and training is undertaken by **Councillors** and that support is provided to them so as to implement this policy.

Users

User Awareness and Training – All users should attend the appropriate training courses. BMSDC and SCC delivers modular training to all users who have access to the Councils' data and network. These training modules inform users of the requirements of the ICT Security Policies. All users must engage with this training and complete all mandatory modules. Corporate Managers have a responsibility to support this training and must raise with HR if any staff member does not or cannot complete the training.

Breach of this Policy – Staff found to be in breach of this policy may be disciplined in accordance with the *Code of Conduct for all employees and Disciplinary Procedure*. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal. It should be noted that breach of the policy could also lead to criminal or civil action if illegal material is involved or legislation is contravened. The Council will not hesitate to bring to the attention of the appropriate Authorities any use of its systems which it believes might be illegal.

Councillors found to be in breach of this policy may be deemed to be a breach of the *Members' Code of Conduct* leading to action by the Corporate Manager – Governance.

Breach of Information Security – Users must report all suspected breaches of information security using the Information Security Incident report form via IT Self Service as soon as they are identified, BMSDC must verify and report incidents to the Information Commissioners Office within 72 hours of being identified to comply with the General Data Protection Regulations.

Appendix 3

GDPR Glossary of Terms

For the purposes of this Regulation:

1. 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

2. processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. ‘filing system’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

7. ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

8. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

9. ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

10. ‘third party’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

11. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

12. ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

13. ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

14. ‘biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

15. ‘data concerning health’ means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

16. ‘main establishment’ means:
    16.1. as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

16.2. as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

17. ‘representative’ means a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation;

18. ‘enterprise’ means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19. ‘group of undertakings’ means a controlling undertaking and its controlled undertakings;

20. ‘binding corporate rules’ means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

21. ‘supervisory authority’ means an independent public authority which is established by a Member State pursuant to Article 51;

22. ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because:

22.1 the controller or processor is established on the territory of the Member State of that supervisory authority
22.2. data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
22.3. a complaint has been lodged with that supervisory authority;

23. ‘cross-border processing’ means either:

23.1. processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

23.2. processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

24. ‘relevant and reasoned objection’ means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union;

25. ‘information society service’ means a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council ([1]);

26. ‘international organisation’ means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.