Medway Council
Data Protection Policy

Document Control

Organisation	Medway Council
Title	Data Protection Policy
Author	Gayle Jones, Information Governance Manager & DPO
Filename	Medway Council Data Protection Policy v1.1
Owner	Data Protection Officer (DPO)
Subject	Data Protection
Protective Marking	Unclassified
Review date	January 2023

Revision History

Revision Date	Revisor	Previous Version	Reason for revision
21/11/18	Gayle Jones	-	Establish policy in line with GDPR & DPA 2018
20/01/21	Heather Corthine	v1.0	Reviewing previous version. Updating GDPR to UK GDPR post Brexit.

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Corporate Management Team	Neil Davies, Chief Executive	06/03/2019
Security & Information Governance Group (SIGG)	Jan Guyler Head of Legal Services – Chair of SIGG	06/03/2019
Senior Information Risk Officer (SIRO)	Perry Holmes, Chief Legal Officer	06/03/2019
Caldecott Guardian	Ian Sutherland,	06/03/2019

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All council employees who handle personal data and Elected Members	All job titles	Via MetaCompliance and/or email
All employees of shared services commissioned by the council who handle personal data of which Medway Council is the data controller.	All job titles	Via agreed process.
Publication on staff intranet and Medway Council public website	N/A	N/A

Contributors

Development of this policy was assisted through information provided by the following organisations:

- Kent County Council

Contents

Introduction

The Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (GDPR)[1] [2] is the law that protects personal privacy and upholds individuals' (sometimes referred to as 'data subjects') rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and processed in accordance with the UK GDPR and current data protection legislation. It will apply to personal information regardless of the way it is used, recorded or stored and whether it is held in paper files or electronically.

Policy objectives

Medway Council (MC) is the Data Controller and as such will comply with its obligations under the DPA[3] and the UK GDPR.[4] MC is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure that its staff and customers are aware of their rights under the legislation.

All staff must have a general understanding of the law and in particular, know how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner, as the Regulator can impose fines of up to £17.5 million for serious breaches of the UK GDPR[5], therefore, it is imperative that MC and all staff comply with the legislation[6]

Scope

'Personal data' is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[7]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identitiy of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the UK GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

MC collects and uses personal information about people for a number of specific lawful purposes as set out in detail in its privacy notice(s). These include carrying out its business and fulfilling its statutory obligations e.g. managing and planning services. Personal information is held on past, current and prospective customers/service users, employees, suppliers and others with whom we communicate.

---

[1] The previous EU Regulation 2016/679

[2] Now the UK GDPR since the UK withdrew from the EU on 31 December 2020. For more information about the the UK GDPR, please follow this link: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

[3] Read the Data Protection Act 2018 in full at the following link: http://www.legislation.gov.uk/ukpga/2018/12/enacted

[4] Read the EU General Data Protection Regulation in full at the following link: https://publications.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

[5] UK GDPR Article 83, figure amended by the DPA 2018 Keeling Schedule

[6] This policy fully reflects the statutory and regulatory guidance provided by the Information Commissioners Office (ICO): https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/ and will be updated in accordance with such guidance as is issued from time to time.

[7] UK GDPR Article 4 Definitions

Correct and lawful treatment of personal information will maintain confidence in MC. Protecting the confidentiality and integrity of personal information is critical.

Roles and responsibilities

The Information Governance Manager, Gayle Jones, is the Data Protection Officer (DPO) and is responsible for informing and advising MC and its staff on its data protection obligations, and for monitoring compliance with those obligations and with its policies.

If you have any questions or comments about:

- the content of this policy,
- if you are likely to process personal information but are unsure of your lawful basis,
- if you need to draft privacy notices,
- if you need assistance dealing with any rights invoked by an individual,
- if you are conducting a DPIA or if you plan any acitivities involving automated decision making,
- if you need help with sharing personal information,
- or if you need further guidance or believe that this policy is not being complied with

you should contact the Data Protection Officer at gdpr@medway.gov.uk

The Assistant Director of Legal and Corporate Services, Perry Holmes, is the Senior Information Risk Owner (SIRO).

The Information Governance Team's primary objective is to facilitate MC's compliance with Information Governance legislation.

All directorates must ensure that all their staff comply with this policy and implement controls to ensure compliance.

All MC staff must ensure they are aware of their responsibilities under the DPA and the UK GDPR and comply with the principles relating to processing of personal information (see section 5 below).[8]

The Principles

The principles set out in the UK GDPR must be adhered to when processing personal information (referred to in the UK GDPR as 'personal data'):

(a) **Lawfulness, fairness and transparency:** Personal data must be processed lawfully, fairly and in a transparent manner).

(b) **Purpose limitation**: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

(c) **Data minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed.

Staff may only process personal information when their role requires it. Staff must not process personal information for any reason unrelated to their role.

[8] For a more detailed explanation of the principles, please follow this link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

(d) **Accuracy:** Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

(e) **Storage limitation:** Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the personal data is processed.

(f) **Integrity and confidentiality:** Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal data are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Transfer limitation

In addition, personal information shall not be transferred to an international organisation or a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information as determined by the European Commission or where the organisation receiving the personal information has provided adequate safeguards[9]. This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer personal information where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal information.

Lawful basis for processing personal information

Before any processing activity starts for the first time, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in MC
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- processing is necessary for compliance with a legal obligation to which MC is subject
- processing is necessary in order to protect the vital interests of the data subject or of another natural person
- processing is necessary for the purposes of the legitimate interests pursued by MC or by a third party[10]
- the data subject has given consent to the processing of his or her personal information for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a

[9] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

[10] The UK GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6(1)(f). However, the ICO indicates that where there are other legitimate purposes outside the scope of its tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

document which deals with other matters, the consent must be kept separate from those other matters.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal information is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

Staff must be satisfied that the processing is necessary for the purpose of the relevant lawful basis (and that there is no other reasonable way to achieve that purpose)

The decision as to which lawful bases or basis applies must be documented, to demonstrate compliance with the data protection principles. Information must be provided about both the purpose(s) of the processing and the lawful basis for it in MC's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside MC's public tasks) a legitimate interests assessment) ('LIA') must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment ('DPIA') may also need to be conducted – see 11. Data Protection Impact Assessments below.

Special Categories of Personal Data

Processing of sensitive personal information (known as 'special categories of personal data' in the UK GDPR) is prohibited[11] unless a lawful special condition for processing is identified.

Special category personal data is information which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, concerns health, a person's sex life or sexiual orientation or is genetic or biometric data which uniquely identifes a natural person.

Special category personal information will only be processed if:

- there is a lawful basis for doing so as identified and;
- one of the special conditions for processing special category personal information applies:
  - (a) the individual has given explicit consent
  - (b) the processing is necessary for the purposes of exercising MC's or an individual's employment, social security or social protection law rights or obligations
  - (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically or legally incapable of giving consent
  - (d) the processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union in relation to its members
  - (e) the processing relates to personal data which are manifestly made public by the data subject
  - (f) the processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
  - (g) the processing is necessary for reasons of substantial public interest
  - (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of of social care and the management of social care systems or services

[11] UK GDPR, Article 9

(i) the processing is necessary for reasons of public interest in the area of public health

(j) the processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes (subject to appropriate safeguards).[12]

In addition, Schedule 1 of the Data Protection Act 2018 sets out further conditions and safeguards which must **additionally** be observed when processing special category data:

The additional conditions are that the processing is necessary for:

1. performing obligations or exercising rights in connection with employment, social security or social protection law
2. health or social care purposes (only under obligation of secrecy)
3. reasons of public interest in the area of public health (and carried out by a health professional)
4. archiving purposes, scientific or historical research purposes or statistical purposes in the public interest
5. specific reasons of 'substantial public interest', which include:

- statutory and government purposes
- equality of opportunity or treatment (this relates to keeping under review the existence or absence of equality of opportunity or treatment between groups of people and does not include: measures or decisions in relation to a specific individual or where the processing causes substantial damage or distress to an individual; or where an individual has written to request the personal information is not processed)
- promoting or retaining racial and ethnic diversity of those holding senior positions in organisations
- preventing or detecting unlawful acts
- protecting the public against dishonesty
- complying with (or assisting others to comply with) a regulatory requirement (e.g.steps to establish whether another person has committed an unlawful act, or been involved in dishonesty, malpractice or other seriously improper conduct)
- preventing fraud
- suspicion of terrorist financing or money laundering in the regulated sector
- provision of confidential counselling and advice (where consent cannot be given or would prejudice the provision of the service)
- safeguarding of children and individuals at risk
- safeguarding of economic well-being of certain individuals
- occupational pensions

Schedule 1 to the DPA sets out in more detail how these conditions are met and these requirements must be carefully considered when considering whether they provide a lawful gateway for processing special category data.

Where MC is relying on certain additional conditions[13] in the DPA as outlined above at 1 (employment etc obligations) or 5 (substantial public interest) or as set out in section 10 below (criminal convictions) the following safeguards must also be in place:

- an appropriate policy document which explains the procedure for complying with the UK GDPR Principles (set out in section 5 above) when relying on these additional conditions

[12] Those safeguards are set out in Article 89, UK GDPR and include organisational and technical measures which include data minimisation and may include pseudonymisation.
[13] Conditions relating to employment, social protection and social security, the substantial public interest conditions and any conditions relating to criminal records as set out in Part 4 of Schedule 1 to the DPA 18.

- an appropriate policy document that explains the retention and erasure of information processed under the additional conditions. (See MC's Retention Schedule in relation to this)
- the policy document(s) must be retained for at least 6 months after processing has ended, regularly reviewed and updated and available to the ICO upon request
- a record must be maintained of the processing of personal data in reliance on these conditions which specifies:
    a) the condition relied on
    b) how it satisfies Article 6 (lawful bases of processing) and
    c) whether personal data is retained and erased in accordance with MC's Retention Schedule and if not, the reasons why.

MC's privacy notice(s) set out the types of special category personal information that it processes, what it is used for, the lawful basis for the processing and any exceptions or conditions that are relied upon.

Special category personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Where explicit consent is required for processing special category personal information, evidence of consent will need to be captured and recorded so that MC can demonstrate its compliance with the law.

Automated Decision Making

Where MC carries out automated decision making (including profiling) it must meet all the principles set out in section 5 above and have a lawful basis for the processing cited in a privacy notice. Explicit consent will ususally be required for automated decision making (unless it is authorised by law or it is necessary for the performance of or entering into a contract).

Additional safeguards and restrictions apply in the case of solely automated decision-making, including profiling. MC must as soon as reasonably possible notify individuals in writing that a decision has been taken based on solely automated processing and that they may, within 1 month of receiving the notification, request reconsideration or a new decision. If such a request is received staff must contact the DPO and MC must reply within 1 month, in certain circumstances the UK GDPR allows an extension of 2 further months[14].

Criminal Records Information

Where criminal offence information relating to convictions, offences or related security measures (including personal information relating to the alleged commission of offences by an individual or proceedings for an offence committed or alleged to have been committed, including sentencing) is processed, a lawful condition for processing that information must also be identified and documented as set out in Schedule 1 of the Data Protection Act 2018. These include:

- consent
- protecting a person's vital interests
- personal data in the public domain

[14] These circumstances can be found at: UK GDPR Article 12(3)

- legal claims
- judicial acts
- any of the conditions listed under substantial public interest
- insurance.

A policy document must also be in place and retained, and a record of processing kept as for special category personal information.

Data Protection Impact Assessments

All MC staff must involve the Information Governance Team at the beginning of any new project that involves the processing of personal data. All data controllers are required to implement 'Privacy by Design' when processing personal information. This means MC processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles (such as data minimisation).

Where processing is likely to result in high risk to an individual's rights and freedoms (for example where a new technology is being implemented or if it will involve large-scale processing of sensitive personal information or information relating to criminal offences) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

During the course of any DPIA, staff should refer to DPIA guidance, seek the advice of the DPO as to whether the DPIA needs to be referred to the ICO and keep it under review throughout the lifetime of the project concerned.

Documentation and records

Written records of processing activities must be kept and should include:

- the name and details of the Directorate and service carrying out the processing
- the purposes of the processing
- the lawful basis for the processing
- a description of the categories of individuals and categories of personal data
- whether personal information of children is being processed
- details of the recipients of personal information
- where relevant, details of transfers to countries outside of the EEA or to international organisations, including documentation of the transfer mechanism safeguards in place
- retention schedules
- a description of technical and organisational security measures in place.

As part of MC's record of processing activities the DPO will document, or link to documention, on:

- information required for privacy notices
- records of consent
- controller-processor contracts
- the location of personal information
- DPIAs and
- records of data breaches.

Records of processing of special category personal information or criminal records information are kept on:

- the relevant purposes for which the processing takes place, including why it is necessary for that purpose
- the lawful basis for processing[15] and
- whether the personal information is retained or erased in accordance with MC's Retention Schedule and, if not, the reasons why.

All Information Asset Owners for UK GDPR should conduct regular reviews of the personal information MC processes within their service and update documentation accordingly. This may include:

- carrying out information audits to find out what personal information is held
- talking to staff about processing activities
- reviewing MC policies, procedures, contracts and agreements to address retention, security and data sharing.

Privacy notices

MC will issue privacy notices from time to time as required, informing individuals about the personal information that it collects and holds and details of how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from individuals, including for HR or employment purposes, the individual shall be given all the information required by the UK GDPR including the identity of the data controller and the DPO, how and why MC will use, process, disclose, protect and retain that personal information through a privacy notice (which must be presented when the data subject first provides the personal information).

When information is collected indirectly (for example from a third party or publically available source) the individual must be provided with all the information required by the UK GDPR as soon as possible after collecting or receiving the personal information and no later than one month from that date. Data collected by a third party must also be obtained in accordance with the UK GDPR and used in a way that is consistent with the proposed use of the personal information set out in the privacy notice.

MC will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Storage limitation

MC maintains a Retention Schedule to ensure personal information is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such personal information to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete from MC systems all personal information that is no longer required in accordance with the Schedule and MC's Records Management Policy. This includes requiring third parties to delete such personal information where applicable.
MC will inform individuals of the period for which personal information is stored and how that period is determined in any applicable privacy notice.

[15] This must include details of which condition is relied on and how the processing satisfies Article 6 of the UK GDPR. [DPA 2018, Schedule 1 Part 4]

Individual rights

Staff as well as any other 'data subjects' have the following rights in relation to their personal information:

- to be informed about how, why and on what basis that information is processed (see MC's privacy statement and privacy notice(s))
- confirmation that personal information is being processed and to obtain access to it and certain other information, via a subject access request
- to have personal information corrected if it is inaccurate or incomplete
- to have personal information erased if it is no longer necessary for the purpose for which it was originally collected/processed or when the consent on which the processing is based has been withdrawn and there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful or where the personal information is no longer needed by MC but the individual requires it to establish, exercise or defend a legal claim, and
- to restrict the processing of personal information temporarily where an individual does not think it is accurate (and MC is verifying whether it is accurate), or where an individual has objected to the processing (and MC is considering whether its legitimate grounds override an indivudal's interests)
- in limited circumstances to receive or ask for their personal information to be transferred to a third party in a structured, commonly used and machine readable format
- where processing of personal information is based on consent, to withdraw that consent at any time
- to request a copy of an agreement under which personal information is transferred outside of the EEA
- to object to decisions based solely on automated processing, including profiling
- to be notified of a data breach which is likely to result in high risk to their rights and obligations
- to make a complaint to the ICO or a Court.

Anyone wishing to exercise any of the rights above, or who receives a request from someone else to exercise any of the rights above, should contact gdpr@medway.gov.uk.

Individual responsibilities

Individuals are responsible for helping MC keep their personal information up to date. Staff can update their own information via the employee self service portal.

Staff may have access to the personal information of other members of staff, suppliers, clients or the public in the course of their employment or engagement. If so, MC expects staff to help meets its data protection obligations to those individuals. For example, staff should be aware that those individuals may enjoy the rights set out above.

If staff have access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes
- only allow other MC staff to access personal information if they have appropriate authorisation
- only allow individuals who are not MC staff to access personal information if they have specific authority to do so
- keep personal information secure (e.g. by complying with the Internet, E-mail and Social Media Policy and Guidelines, with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with MC's Information Security Policy and Records Management Policy)

- not remove personal information, or devices containing personal information (or which can be used to access it) from the council's premesis unless appropriate security measures are in place (such as pseudonymisation or encryption) to secure the information and the device; and comply with MC's ICT Security Policy.
- not store personal information on local drives or on personal devices that are used for work purposes and comply with the council's ICT Security Policy.

Information security

MC will use appropriate technical and organisational measures in accordance with its Information Security Policy to keep personal information secure, and in particular, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Staff are responsible for keeping information secure in accordance with the Information Security Policy and must read that policy in conjunction with this one.

MC will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal information that it owns or maintains on behalf of others and identified risks (including the use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

All staff are responsible for protecting the personal information MC holds. Staff must guard against unlawful or unauthorised processing of personal information and against the accidental loss of, or damage to, personal information. Staff must exercise particular care in protecting sensitive special category personal information from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal information from the point of collection to the point of destruction. Staff may only transfer personal information to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the confidentiality, integrity, resilience[16] and availability of the personal information, defined as follows:

(a) confidentiality means that only people who have a need to know and are authorised to use the personal information can access it

(b) integrity means that personal information is accurate and suitable for the purpose for which it is processed

(c) availability means that authorised users are able to access the personal information when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards MC has implemented and maintains in accordance with the UK GDPR.

Where MC uses external organisations to process personal information on its behalf, additional security arrangements must be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may only act on the written instructions of MC
- those processing personal information are subject to the duty of confidence

[16] Article 32(1)(b) includes resilience. This is the ability of systems to continue operating under adverse conditions and an organisation's ability to restore them to an effective state.

- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of MC and under a written contract
- the organisation will assist MC in allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to MC as requested at the end of the contract
- the organisation will submit to audits and inspections, provide MC with whatever information it needs to ensure that both parties are meeting their data protection obligations, and tell MC immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms from Legal Services.

Storage and retention of personal information

Personal information will be kept securely in accordance with MC's information security policies and data protection obligations.

Personal information must not be retained for any longer than necessary. The length of time personal information should be retained will depend upon the circumstances, including the reasons why personal information was obtained. Staff should adhere to MC's Records Management Policy with reference to its Retention Schedule.

Personal information that is no longer required will be deleted permanently from MC's information systems and any hard copies will be destroyed securely.

Data breaches

A data breach may take many different forms:

- loss or theft of data or equipment on which personal information is stored
- unauthorised access to or use of personal information either by a member of staff or third party
- loss of data resulting from an equipment or systems (including hardware or software) failure
- human error, such as accidental deletion or alteration of data or emailing the wrong individual or pressing 'reply all' instead of 'reply'
- unforeseen circumstances, such as a fire or flood
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- blagging offences where information is obtained by deceiving the organisation which holds it

If MC becomes aware of a data breach that is likely to result in a risk to individuals' rights, it must report it to the ICO within 72 hours (where possible), but in any event, without undue delay. MC will also notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

Staff must inform their service manager immediately if a data breach is discovered and make all reasonable efforts to recover any information. Staff and managers must have regard to MC's Data Breach Policy.

Training

MC will ensure that staff are adequately trained regarding their data protection responsibilities. All staff are required to complete mandatory information governance and data protection training every two years.

Consequences of a failure to comply

MC takes compliance with this policy very seriously. Failure to comply puts data subjects at risk and carries the risk of significant civil and criminal sanctions for the individuals responsible and for MC and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under MC's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If staff have any questions or concerns about this policy they should contact their line manager or the Data Protection Officer.

Review of policy

This policy will be reviewed on an annual basis and updated as necessary. A copy of the versions of this policy will be retained so that it is available to the ICO if requested.

Related policies/guidance

This policy should be used in conjunction with the following related policies/guidance:

- Information Governance Policy
- Data Breach Policy
- Information Security Policy
- Information Sharing Policy
- Anonymisation/Pseudonymisation Policy
- Records Management Policy
- Kent and Medway Information Sharing Agreement
- ICT Security Policy
- Flexible Working Policy
- Internet, Email & Social Media Policy
- Remote Working
- Use Your Own Device Policy (Annex to ICT Security Policy)
- ICT's Security Information pages on Service Desk Portal

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The UK GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data 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. It is responsible for establishing practices and policies in line with the UK GDPR. Medway Council is the Data Controller of all personal information relating to its clients, customers and staff.

Data Subject: a living, identified or identifiable individual about whom MC holds Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of **Privacy by Design** and should be conducted for all major systems or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the UK GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

UK General Data Protection Regulation (UK GDPR): the UK General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the UK GDPR.

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

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.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR such that necessary safeguards are integrated into the processing from the outset.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when MC collects information about them. These notices may take the form of general **privacy** statements applicable to a specific group of individuals (for example,

employee **privacy** notices or the website **privacy** policy) or they may be stand-alone, one time **privacy** statements covering Processing related to a specific purpose.

Processing: means anything done with 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.

Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation: means processing 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.

Special Categories of Personal Data: information 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.