MoleValley District Council

Agenda Item 11

Executive Member	Councillor Metin Huseyin, Executive Member for Finance and Corporate Services
Strategic Management Team Lead Officer	Patrick McCord, Interim Corporate Head of Service
Author	Chris Harris, Legal Services Manager
Telephone	01306 879130
Email	Chris.harris@molevalley.gov.uk
Date	23/02/2018

Ward (s) affected	All	**Key Decision**	No

Subject	**Adoption of new Data Protection Policy**

Recommendations

1. That the Data Protection Policy be adopted from a date to be determined by the Council's Chief Executive
2. That authority be delegated to the Data Protection Officer in consultation with the Executive Member to implement further GDPR relevant policies and to make amendments to the Policy to enable the Council to make further progress in respect of measures that will improve GDPR compliance by the Council.
3. That authority be delegated to Information Asset Owner for HR in consultation with the Data Protection Officer and the Executive Member to implement a specific GDPR compliant HR policy (save where any aspect of the same already falls within the remit of the Head of Paid Service).

Executive Summary

The General Data Protection Regulations (GDPR) will require all bodies who handle data in some way to be compliant with the provisions of the regulation by 25 May 2018.

A project has been running since August 2017 to ensure that the Council has the necessary policies and procedures in place.

The annexed Data Protection Policy is recommended for adoption by the Council to ensure it satisfies this obligation as a data controller under GDPR. The main changes between the Data Protection Act and the GDPR are:

1) The Accountability principle imposes new obligations. The Council will not only need to comply with the requirements of new data protection legislation, but must be able to show how it is compliant with all of the requirements of the GDPR, for example by keeping comprehensive records of both the range of processing by the Council and how risks have been identified and, if appropriate, mitigated.
2) The requirement for registration of the range of MVDC's data processing functions with the ICO has been removed, though a (higher) fee will still be payable to the ICO.
3) The appointment of a Data Protection Officer is now a statutory obligation, with specific requirements and protections.
4) Two conditions that were used frequently under the Data Protection Act to satisfy

the requirement for personal data to be processed in accordance with the first data protection principle (re fair and lawful processing) – ie, consent and legitimate expectation – will have significant limitations placed on their use in future.

5) Further information will need to be provided to data subjects to improve transparency.

6) Protection of the personal information of data subjects will have to be built into processes and systems – "data protection by design and default"

7) The maximum fines which can be imposed for breaches will significantly increase

8) Tighter rules will apply re data breach reporting so more breaches will need to be reported to the ICO than was the case under the Data Protection Act.

9) Due to specific requirements that will relate to the Council in its capacity as employer, a separate HR specific policy will be implemented in due course

In addition, please note that personal data regarding law enforcement is excluded from the GDPR, but any new legislation is also likely to give statutory force to the Law Enforcement Directive.

Corporate Priority Outcomes

Community Wellbeing

Active communities and support for those who need it

- Improve opportunities for residents to live safe and healthy lives

The Executive has the authority to determine the Recommendations

1. Background

1.1 General Data Protection Regulation (GDPR), was published on 4 May 2016 and EU organisations will have to comply with its provisions by 25 May 2018. Many of the data protection principles in the new legislation are much the same as those in the current Data Protection Act (Act)

1.2 The GDPR will introduce several new concepts and approaches, the most significant of which are outlined below. The GDPR is also designed to be more future-proof and forward-looking than the Data Protection Act.

1.3 Many of the principles in the new legislation are much the same as those in the Act, (although there is a new Data Protection Bill, which is currently before Parliament and is likely to receive Royal Assent at the end of March). The indication is that if an organisation has measures in place to comply with the Act then that is a strong starting point to build from. There are some important new elements and some things will need to be done differently.

1.4 While GDPR will apply to the vast majority of personal data processed by the Council it will not apply to the processing of personal data relating to criminal convictions and offences. It is likely that any new Data Protection Act that will implement the provisions of the GDPR into law will have very similar provisions for processing personal data relating to criminal convictions and offences as set out in the Law Enforcement Directive.

2. Key Provisions

Harmonisation across and beyond the EU

2.1 The GDPR is intended to establish one single set of rules across Europe which EU policy makers believe will make it simpler and cheaper for organisations to do business across the Union.

What is "Personal Data"?

2.2 "Personal data" is defined in the GDPR as any information relating to an person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

2.3 So online identifiers including an IP address, cookies and so forth will now be regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject.

2.4 "Sensitive personal data", is defined as "special categories" of personal data in the future, is defined as 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.

2.5 There is no distinction between personal data about individuals in their private, public or work roles – the person is the person.

Controllers and Processors

2.6 The GDPR separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide "sufficient guarantees to implement appropriate technical and organisational measures" to meet the Regulation's requirements and to protect data subjects' rights.

2.7 Controllers and processors are required to "implement appropriate technical and organisational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals."

2.8 The GDPR provides specific suggestions for what kinds of security actions might be considered that are appropriate to the risk, including:

- The pseudonymisation and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2.9 Controllers and processors that adhere to either an approved code of conduct or an approved certification may use these tools to demonstrate compliance.

2.10 The controller - processor relationships must be documented and managed with contracts that mandate privacy obligations – ultimately controllers must assure themselves of a processor's privacy capabilities.

Fines and Enforcement

2.11 There will be a substantial increase in fines for organisations that do not comply with the GDPR.

2.12 Regulators will now have authority to issue penalties equal to the greater of €10 million (though this will be the maximum for the Council) or 2% of the entity's global gross revenue (the higher amount being relevant for companies wholly or partly owned by the Council) for violations of, for example: the requirement to integrate data protection into systems and projects by design and by default; record-keeping; security; breach notification; and privacy impact assessment obligations.

2.13 However violations of obligations related to legal justification for processing, for example including the data protection principles, conditions for lawfulfulness of processing (including consent), data subject rights, and cross-border data transfers may result in penalties of the greater of €20 million (again, the maximum for the Council) or 4% of the entity's global gross revenue (in the case of wholly or partly owned companies).

2.14 It will remain to be seen how the supervisory authority tasked with imposing these fines will work, though it can probably be assumed that the seriousness of the breach is likely to be measured by reference to things such as: the gravity of the offence and how long it has been going on; any intentional or negligent conduct; the level of damage suffered by data subjects; what technical and organisational measures were in place; and whether there have been previous infringements.

Data Protection Officers

2.15 Data Protection Officers must be appointed for all public authorities.

2.16 The regulation requires that they have "expert knowledge of data protection law and practices." The level of which "should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor."

2.17 The data protection officer's tasks are also delineated in the regulation to include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance including managing internal data protection activities, training staff and members, and conducting internal audits.
- Advising with regard to data protection impact assessments when required
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.

- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten, and related rights.

2.18 Data Protection Officers may insist upon additional resources to fulfil their job functions and for their own ongoing training.

2.19 They must have access to the company's data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line "to the highest management level" of the company.

2.20 Data Protection Officers are expressly granted significant independence in their job functions but may perform other tasks and duties provided they do not create conflicts of interest.

2.21 The GDPR expressly prevents dismissal or penalty of the data protection officer for performance of his/her tasks and places no limitation on the length of this tenure.

2.22 The GDPR also allows the data protection officer functions to be performed by either an employee of the controller or processor or by a third party service provider.

Privacy Management

2.23 GDPR requires a risk-based approach to ensure appropriate technical and organisational controls are developed according to the degree of risk associated with the processing activities.

2.24 Where appropriate, privacy impact assessments must be made – with the focus on protecting data subject rights.

2.25 Data protection safeguards must be designed into services from the earliest stage of development – Privacy by Design and Default.

2.26 Privacy-friendly techniques such as pseudonymisation will be encouraged to reap the benefits of big data innovation while protecting privacy.

2.27 There is an increased emphasis on record keeping for controllers – the accountability principle - designed to help demonstrate and meet compliance with GDPR and improve the capabilities of organisations to manage privacy and data effectively. Appropriate corporate governance will be of even greater significance with GDPR than with the Act.

Consent

2.28 Under the first data protection principle (ie, the requirement for fair, lawful and transparent processing), consent is one of several conditions which has to be satisfied to make the processing fair and lawful.

2.29 The other conditions are that: (i) the processing is necessary for compliance with a legal obligation, (ii) the processing is necessary to protect the vital interests of the data subject, (iii) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and (iv) that the processing is necessary for the purposes of the legitimate interests pursued by the data controller (though local authorities will have strict limitations placed on their use of this).

2.30 According to the GDPR consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a

statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;"

2.31 The purposes for which the consent is gained needs to be "collected for specified, explicit and legitimate purposes". This means that it needs to be obvious to the data subject what their data is going to be used for at the point of collection.

2.32 Consent should be demonstrable – in other words organisations need to be able to show clearly how consent was gained and when.

2.33 Consent must be freely given – a controller cannot insist on data that is not required for the performance of a contract as a pre-requisite for that contract.

2.34 Withdrawing consent should always be possible – and should be as easy as giving it. It will not therefore be appropriate for the majority of processing by the Council.

2.35 If consent is required for the processing of personal data involving children under 13 years of age, then it must be given by a person with parental responsibility for the child,

Information Provided at Data Collection

2.36 The information that must be made available to a data subject when data is collected from the data subject has been strongly defined and includes;

- the identity and the contact details of the controller and DPO
- the purposes of the processing for which the personal data are intended
- the legal basis of the processing.
- where applicable the legitimate interests pursued by the controller or by a third party;
- where applicable, the recipients or categories of recipients of the personal data;
- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
- where applicable, if a transfer to a third country is intended;
- the existence of the right to access, rectify or erase the personal data;
- the right to data portability;
- the right to withdraw consent at any time;
- and the right to lodge a complaint to a supervisory authority;

2.37 Importantly, where the data has not been obtained directly from the data subject – perhaps using a third party list – the list also includes:

- from which source the personal data originate.
- the existence of any automated decision making/ profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2.38 There are some exceptions – notably where the effort would be disproportionate (although this is unlikely be a good justification in day to day circumstances) and, importantly, where the information has already been provided to the data subject.

Profiling

2.39 The regulation defines profiling as any automated processing of personal data to determine certain criteria about a 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".

2.40 With the exceptions set out in the paragraph immediately below, individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on him/her or otherwise significantly affects them. So, individuals can opt out of profiling.

2.41 Automated decision making will be legal where individuals have **explicitly** consented to it, or if profiling is necessary under a contract between an organisation and an individual, or if profiling is necessary for compliance with a legal obligation, or necessary in order to protect the vital interests of a data subject or other natural person. This means, for example, that individuals cannot opt out of profiling where the Council is under a legal duty in respect of the processing.

Breach & Notification

2.42 According to the regulation a "personal data breach" is "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".

2.43 The wilful destruction or alteration of data is as much a breach as theft.

2.44 With the exception set out below, in the event of a personal data breach data controllers must notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. If notification is not made within 72 hours, the controller must provide reasons for the delay.

2.45 Notice is not required if the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals. It is not clear, at this stage, how this will be interpreted.

2.46 Importantly when a data processor experiences a personal data breach, it must notify the controller but otherwise has no other notification or reporting obligation.

2.47 Should the controller determine that the personal data breach is likely to result in a high risk to the rights and freedoms of individuals, it must also communicate information regarding the personal data breach to the data subjects affected. Again, this must be done without undue delay.

2.48 The GDPR provides exceptions to this requirement to notify data subjects in any of the following circumstances:

1. The controller has implemented appropriate technical and organisational protection measures that render the data unintelligible to any person who is not authorised to access it, such as encryption.
2. The controller takes actions subsequent to the personal data breach to ensure that the high risk for the rights and freedoms of data subjects is unlikely to materialise.
3. When notification to each data subject would involve disproportionate effort, in which case alternative communication measures may be used.

Data Subject Access Requests

2.49 Data controllers will have to provide Individuals with more information on how their data is processed and this information should be available in a clear and understandable way.

2.50 Where requests to access data are manifestly unfounded or excessive, organisations will be able to charge a fee for providing access.

2.51 DSAR's must be executed "without undue delay and at the latest within one month of receipt of the request."

2.52 Subject access requests must also give all the information relating to purposes for collection that should have been provided upon collection.

The Right to Data Portability

2.53 This right is clearly focused on helping drive competition between commercial service providers and seeks to drive automated transfers of data (using a common format yet to be defined) between services which primarily process customers automatically – so, for example, these could include utilities, banks, telecoms and ISP's.

Retention & The Right to be Forgotten

2.54 As noted above, controllers must inform subjects of the period of time (or reasons why) data will be retained on collection.

2.55 Should the data subject subsequently wish to have their data removed and the data is no longer required for the reasons for which it was collected then it must be erased.

3. Options

3.1 **Option 1:** To approve the adoption of the new Data Protection Policy, subject to the Data Protection Officer being authorised to make amendments to the Policy in consultation with the Executive Member to take account of any changes to legislation or guidance.

3.2 **Option 2:** Not to approve the Policy and continue with the existing Policy.

3.3 **Option 3:** To suggest amendments to the proposed new Data Protection Policy.

4. Corporate Implications

Financial Implications

4.1 The costs of seeking compliance so far has been contained within existing budgets but it is noted that GDPR requires the Council to provide the Data Protection Officer with the resources necessary to fulfil the tasks associated with the role. As a result more resources may be required as matters progress. Given the maximum fines will increase substantially, it is noted that there may be highly significant consequences of failure to comply with GDPR

Legal Implications

4.2 All organisations which handle personal data in some way must be compliant with the requirement of the GDPR by 25 May 2018

Monitoring Officer commentary

4.3 The Monitoring Officer is satisfied that all relevant legal implications have been taken into account.

S151 Officer commentary

4.4 The s151 Officer is satisfied that all relevant financial implications have been taken into account in connection with this policy.

Risk Implications

4.5 Failing to implement GDPR across the Council could result in enforcement action being taken by the Information Commissioner's Office against the Council, including the imposition of a fine.

4.6 Option 1 is the preferred option, unless members believe substantive changes are required, in which case option 3 will need to be considered. Option 2 is not recommended because the current Data Protection Policy is not GDPR compliant.

4.7 It is noted that the ICO has indicated that provided organisations are genuinely attempting to be compliant, then they see their role as helping them to achieve compliance through advice and assistance.

Equalities Implications

4.8 The new data protection framework further protects data subjects and the processing of personal data that would reveal protected characteristics. It is possible it will serve to promote equality, particularly given that data subjects will benefit from strengthened rights.

Employment Issues

4.9 The implementation of the GDPR has major implications for all employers and will therefore require agreement and adoption of a specific [HR data protection policy].

4.10 It should also be noted that some additional resources may be required to assist the Data Protection Officer.

Sustainability Issues

4.11 No sustainability issues have been identified

Consultation

4.12 None

Communications

4.13 None

Background Papers

4.14 None

1. Introduction

1.1 Background to the General Data Protection Regulation ('GDPR')
The purpose of the General Data Protection Regulation 2016 is to better protect the "rights and freedoms" of natural persons (i.e. living individuals). The GDPR sets out both a new legal framework and more specific requirements regarding the processing of personal data about MVDC's residents (and all those whose personal data is processed by MVDC). While these requirements correspond well with MVDC's core values, there are some fundamental changes that will need to be made to the way in which MVDC processes personal data. All staff will therefore need to be aware of, and take responsibility for all changes required as a result of any new or ongoing GDPR requirements that are relevant to their working practices.

For the avoidance of doubt, subject to adoption by the appropriate persons, the relevant aspects of this policy will until further notice also apply to data processing functions by, or for and on behalf, the following data controllers:

- The Electoral Registration Officer/ Returning Officer,
- Mova Property Limited,
- Mova Holdings Limited, and
- Members (when acting as representatives for members of their ward – ie, not when acting for their political party)

In addition to this Policy, MVDC has specific obligations in relation to its functions as an employer which will be covered by an additional policy – to be implemented in due course.

1.2 Scope of the GDPR principles
Material scope (Article 2) **–** the GDPR applies to the processing of personal data wholly or partly by automated means (i.e. decisions made by a computer algorithm or similar) and to the processing, other than by automated means, of personal data (i.e. paper records, or electronic records held on databases or document management systems) that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) **–** the GDPR will apply to MVDC because MVDC is a data controller established in the EU (European Union). Please contact the Data Protection Officer if you become aware of any processing of personal data outside of the EU without appropriate safeguards being in place.

1.3 Article 4 definitions

Personal data – 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.

Special categories of personal data – 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.

Data controller – 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 the EU or Member State law, or the controller or the specific criteria for its nomination may be provided for by EU or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Information Asset Owner – the relevant member of the Business Management Team (or otherwise if another person has been delegated as an Information Asset Owner) who has responsibility for the personal information stored within their service area.

Processing – 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, storing, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling **–** is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. (This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.)

Personal data breach **–** 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. There is an obligation on the controller to report the majority of personal data breaches to the Information Commissioner's Officer without undue delay (defined as 72 hours at the latest from becoming aware of it)

Data subject consent **-** 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.

Mole Valley District Council

Insert Company Logo

Child – a child under 13 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Subject Access Request Procedure – MVDC's procedure for responding to subject access requests as set out at Annexe 2

Third party – 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.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Policy statement

2.1 MVDC is committed to compliance with [the General Data Protection Regulation and Law Enforcement Directive/ Data Protection Act 2018] in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information MVDC collects and/ or processes in accordance with the GDPR and all relevant Acts of parliament.

2.2 Compliance with the GDPR is described by this policy in conjunction with other relevant policies and procedures such as the Information Security Policy.

2.3 This policy applies to all of MVDC's personal data processing functions, including those performed on residents, customers', clients', suppliers' and partners' personal data, and any other personal data MVDC processes from any source whatsoever. The only caveats to this relate to (i) instances where MVDC processes personal data for and on behalf of third parties, in which case please refer to the relevant contract terms to determine which policies' apply, and (ii) MVDC's HR functions in respect of its employees. For the avoidance of doubt, when personal data is processed for and on behalf of MVDC in its capacity as an employer this policy will be construed by reference to the relevant requirements of MVDC's [HR data protection Policy].

2.4 All staff with responsibility for relevant registers and policies must liaise with the Data Protection Officer on an annual basis to determine whether any changes need to be made to those policies.

2.5 This policy (together with any other relevant MVDC data protection policies for any particular type of processing) applies to all Employees/temporary or permanent Staff / Contractors and any other persons processing personal data for and on behalf of MVDC (whether as Data Controller or Data Processor - unless a different policy is in force and signed up to in respect of information processed pursuant to any MVDC data processing agreements). Any breach of the GDPR as set out in this and other relevant policies will be dealt with under MVDC's disciplinary policy and may also be a criminal offence.

Mole Valley District Council

Insert Company Logo

2.6 Partners and any third parties working with or for MVDC, and who have or may have access to personal data, will (unless any departure is first agreed with the Data Protection Officer) be expected to have read, understood and agreed to comply with this policy. No third parties shall be provided with access to personal data held by MVDC without also having first entered into any other appropriate agreements (eg, a confidentiality agreement).

3. Responsibilities and roles under the General Data Protection Regulation

3.1 The majority of personal data processed by MVDC will be processed by it in its capacity as a data controller (or, for example, for certain shared working arrangements, as one of two or more data controllers) under the GDPR. Personal data, however, that is processed by MVDC acting for and on behalf of third parties, will be processed by MVDC in its capacity as a data processor.

3.2 The Business Management Team and all others in managerial or supervisory roles throughout MVDC are responsible for encouraging good information handling practices within MVDC; responsibilities for compliance with this and other relevant policies are set out in individual job descriptions.

3.3 MVDC's Data Protection Officer (a new statutory position) will be a member of, or directly report into the senior management team, and will be accountable to the Chief Executive of MVDC for the management of personal data within MVDC, and also for ensuring that compliance with data protection legislation and good practice can be demonstrated. With the exception of information technology security, the joint responsibility for which will rest with the Corporate Head for ICT, this accountability includes:

3.3.1 development and implementation of GDPR compliant policies (in consultation with others where appropriate); and

3.3.2 security and risk management (in consultation with Information Asset Owners and Executive Head for ICT) in relation to compliance with this policy.

3.4 The Data Protection Officer has been appointed to take responsibility for MVDC's compliance with this policy on a day-to-day basis and, moreover, has overall responsibility for ensuring that MVDC complies with the GDPR.

3.5 The Data Protection Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and can be consulted by staff seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all MVDC staff and others who are required to comply with this policy.

3.7 MVDC staff are responsible for ensuring that any personal data about them and supplied by them to MVDC is accurate and up-to-date.

4. Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. MVDC's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing". The conditions for processing are, one of which must first be satisfied, are:

1) Consent by the data subject,
2) That the processing is necessary for the performance of a contract to which the data subject is a party (or to take steps at the request of the data subject prior to entering into a contract),
3) The processing is necessary in order to comply with a legal obligation,
4) The processing is necessary in order to protect the vital interests of either the data subject or another person,
5) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and
6) The processing is necessary for the purposes of the legitimate interests pursued by the data controller (though note because the circumstances in which MVDC will be able to use this are very limited this condition should not be used without the prior agreement of the Data Protection Officer or in accordance with any MVDC policy subsequently distributed).

If you are processing personal data where MVDC is under a statutory duty to do so, for example, then the processing will automatically be fair and lawful. Though the processing must then also comply with all other principles. All staff must be familiar with the legislation that sets out the nature of the powers and duties which they are processing the personal data under.

Fairly – one example of fair processing is that certain information must be made available to the data subjects. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The GDPR has increased requirements about what information should be available to data subjects, which is covered in the 'Transparently' requirement.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.
MVDC's Privacy Notice Procedure and its general Privacy Notice (as may be amended) are set out in the relevant pages on the GDPR section on MOLLY [to follow]. Information Asset Owners are responsible for ensuring their privacy notices, or other method of communicating this information to data subjects, are GDPR compliant.

Mole Valley District Council

Insert Company Logo

Where MVDC is the data controller, the specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 the identity and the contact details of MVDC (as the data controller) and, if any, of the controller's representative;
4.1.2 the contact details of the Data Protection Officer;
4.1.3 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4.1.4 the period for which the personal data will be stored (and which may be by reference to MVDC's data retention policy);
4.1.5 the existence of the rights (where applicable) to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights;
4.1.6 the categories of personal data concerned;
4.1.7 the recipients or categories of recipients of the personal data, where applicable;
4.1.8 where applicable, that the controller intends to transfer personal data to a recipient in a non EU country and the level of protection afforded to the data;
4.1.9 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit and legitimate purposes
Personal data obtained for specified purposes must not be used for a different purpose unless that different purpose is itself in compliance with MVDC's data protection or other relevant policies.

4.3 Personal data must be adequate, relevant and limited to what is necessary for processing

4.3.1 Although overall responsibility for ensuring that MVDC does not collect information that is not strictly necessary for the purpose for which it is obtained rests with the Data Protection Officer, all staff are responsible for the personal data collected by them (under their contracts of employment)
4.3.2 All data collection forms (electronic or paper-based), including personal data collection requirements in new information systems, must include a fair processing statement or, if appropriate, a link to the relevant privacy statement/ Fair Processing Notice.
4.3.3 The Data Protection Officer will ensure that all data collection methods are reviewed by *[internal audit]* at periodic intervals to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay (where appropriate)

4.4.1 Personal data that is stored by MVDC must be reviewed and updated as necessary. No personal data should be kept unless it is reasonable to assume that it is accurate.
4.4.2 Data subjects should be made aware how they can inform MVDC of corrections to their personal data when it becomes inaccurate or out of date.
4.4.3 The Data Protection Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up

to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors. If insufficient procedures and policies are in place in any service area it is the responsibility of the relevant Information Asset Owner to inform the Data Protection Officer of this.

4.4.4 On at least an annual basis, the Information Asset Owners will review the retention dates of all the types of personal data processed by MVDC, by reference to the information asset and other relevant registers, and will arrange for the identification of any data that is no longer required in the context of the registered purpose. The Information Asset Owners will then oversee the secure deletion /destruction of the personal data in line with the appropriate MVDC policy/ policies.

4.4.5 The Data Protection Officer [or Information Asset Owner as appropriate] is responsible for responding to requests for rectification from data subjects without undue delay. If MVDC decides not to comply with the request, for example because it is under a legal obligation to do the processing, or is processing the information to perform a task carried out in the public interest or in the exercise of official authority vested in the data controller, MVDC's response will set out both the reasoning for its decision, and also inform the data subject of their right to complain to the supervisory authority and seek judicial remedy.

4.4.6 The Data Protection Officer, following consultation with the Information Asset Owner is responsible for making appropriate arrangements, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is permitted.

4.5 <u>Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.</u>

4.5.1 Personal data will be retained in line with MVDC's Records Retention Policy (as amended from time to time) and, once its retention date has passed, it must be securely destroyed (and for the avoidance of doubt Information Asset Owners will arrange for secure destruction by any third party applications providers.

4.5.2 Where personal data is to be, or has been retained beyond the relevant retention period, this must be justified by the Information Asset Owner, and, where reasonably practicable, it will be minimized, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach. The justification for any such retention must be considered in line with data protection legislation. Any continued retention should be justified in writing.

4.6 <u>Personal data must be processed in a manner that ensures appropriate security measures are in place</u>

The Data Protection Officer, with the assistance of the relevant Information Asset Owners (and ICT lead contact, where appropriate) will carry out a risk assessment

taking into account all the circumstances of MVDC's controlling or processing operations.

The Data Protection Officer should also consider the extent of possible damage or loss that might be caused to individuals if a security breach occurs, the effect of any security breach on MVDC itself, and any likely reputational damage including the possible loss of trust in MVDC by its residents.

When assessing appropriate technical measures, the Executive Head with responsibility for ICT will report to the Data Protection Officer on all relevant matters ICT retains corporate responsibility for.

When assessing appropriate organisational measures the Data Protection Officer, in consultation with the relevant information asset owner or other appropriate person, will consider the following:

- The appropriate training levels throughout MVDC;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable cabinets;
- Restricting the use of portable electronic devices outside of the workplace other than as permitted pursuant to MVDC's ICT Security Policy;
- Restricting the use of employee's own personal devices in accordance with the ICT Security policy;
- Adopting clear rules about passwords;
- The imposition of contractual obligations on any relevant organisations, requiring them to take appropriate security measures if transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 <u>The controller must be able to demonstrate compliance with all requirements under the GDPR (accountability)</u>

The GDPR includes provisions that promote accountability and good governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires MVDC to demonstrate that it complies with the principles.

MVDC will demonstrate compliance with the data protection principles by

- implementing appropriate technical and organisational measures that ensure and demonstrate that compliance. This will include, for example, internal data protection policies, staff and member training, internal audits of processing activities, and internal HR policies;
- maintaining relevant documentation on processing activities;
- appointing a data protection officer;
- implementing measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - data minimisation;
    - pseudonymisation;
    - transparency;
    - creating and improving security features on an ongoing basis.
- using data protection impact assessments where appropriate.

5. Data subjects' rights

5.1 Data subjects have the following rights regarding data processing, and the personal data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of personal information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

5.1.5 To not have significant decisions that will affect them taken solely by automated process.

5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

5.1.7 To take action to rectify, block, erase, or destroy inaccurate data.

5.1.8 To request MVDC to assess whether any provision of the GDPR has been contravened.

5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another data controller.

5.1.10 To object to any automated profiling that is occurring without consent.

All staff and others reasonably requested to do so will assist with any Subject Access Requests or other requests from or involving data subjects in a timely manner (including without limitation complaints made to the Information Commissioner's Office).

6. Consent

Mole Valley District Council

Insert Company Logo

6.1 In respect of consent being used as one of the conditions to show the processing by MVDC is fair and lawful (ie, to satisfy the first data protection principle), new restrictions are in place which will mean it will not be possible for MVDC to use consent as an appropriate condition for the vast majority of its processing in future

6.2 MVDC and its staff and all others required to comply with this policy understand 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Please note that if consent is used as the basis for processing then the data subject can withdraw their consent at any time.

6.3 All relevant persons must also understand, before using 'consent' as the basis of processing that is will mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information or required as a precondition for entering into a contract will not be compliant and so cannot be used a valid basis for processing.

6.4 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. Information Asset Owners must be made aware, and ensure records are kept of, processing functions where consent is used as the lawful basis for the processing.

6.5 If consent is used for the processing of sensitive personal data, explicit written consent of data subjects must be obtained

6.6 Where MVDC provides online or other services to children, then parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

6.7 Where opt in boxes are used for any reason, they must not be pre ticked.

7. Security of data

7.1 All employees/ temporary or permanent staff/ contractors and any other persons exercising personal data processing functions are responsible for ensuring that any personal data that MVDC holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that disclosure is permitted under the GDPR and in accordance with this and any other relevant policies. Where appropriate, the third party/ parties to whom personal data are disclosed should enter into a confidentiality agreement. Any data to be transferred must be encrypted and any transfer of data must be done securely.

7.2 All personal data should be accessible only to those who reasonably need to use or otherwise access it in accordance with this policy. All personal data should be treated as an information asset and where appropriate kept:

- in a lockable room or other area (with controlled access if appropriate); and/or
- in a locked drawer or filing cabinet; and/or
- Any data at rest must be encrypted and protected by password policy.

7.3 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without authorisation.

Mole Valley District
Council

Insert
Company
Logo

Manual records must be placed on the relevant file as soon as reasonably practicable following their preparation.

7.4 Personal data may only be deleted or disposed of in line with the Records Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed as required by MVDC's Data Security – Equipment Disposal policy before disposal.

7.5 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff with authority to process personal information off site must be particularly vigilent

8. Disclosure of data

8.1 Employees/temporary or permanent Staff / Contractors and any other persons processing personal data for and on behalf of MVDC (whether as data controller or data processor) must ensure that personal data is not disclosed to unauthorised third parties. It is the disclosing individual's responsibility to ensure that no such disclosures take place without first ensuring that there is a legal pathway permitting the disclosure. Particular care should be taken with non routine processing to third parties. Where there is a sufficient pathway permitting the processing, it is also important to ensure that additional personal information is not disclosed that is in excess of that reasonably needed for the task it was collected for.

8.2 When considering requests to disclose personal data, please ensure appropriate records are made and retained.

9. Retention and disposal of data

9.1 Subject to paragraph 9.2 below, MVDC shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary in the circumstances, in relation to the purpose(s) for which the data was originally collected.

9.2 MVDC may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data will be set out in MVDC's Records Retention Policy (as amended).

9.4 Employees/temporary or permanent Staff / Contractors and any other persons processing personal data for and on behalf of MVDC must, unless they have express authorisation to retain it for longer, dispose of it as set out in MVDC's Records Retention Policy.

9.5 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects - as communicated to staff from time to time).

Mole Valley District
Council

Insert
Company
Logo

10. Data transfers

10.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

10.1.1 An adequacy decision
A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union*. *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

10.1.2 Privacy Shield
If MVDC wishes to transfer personal data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce

All contracts or other processing involving international transfers of personal data outside the EEA should be discussed with the Data Protection Officer prior to the processing.

11. Information asset register/data inventory

11.1 MVDC has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. MVDC's data inventory and data flow determines

- business processes that use personal data;
- source of personal data;
- volume of data subjects;
- descriptions of of personal data processed;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Organisation Name throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

11.2 It is important that relevant staff are aware of any risks associated with the processing of particular types of personal data.

Mole Valley District Council

Insert Company Logo

11.2.1 Employees/temporary or permanent Staff / Contractors and any other persons processing personal data for and on behalf of MVDC shall inform the relevant Information Asset Owner at the earliest opportunity when a project is planned that involves the processing of personal data. The Information Asset Owner will then consult with the project manager to consider how the risks should best be identified, and where necessary, minimised to an acceptable level. Privacy by design principles will be considered at the outset. Data protection impact assessments (DPIAs) must be carried out in relation to all high risk processing of personal data by MVDC, and in relation to processing undertaken by other organisations on behalf of MVDC.

11.2.2 The project manager shall liaise with the Data Protection Officer and any relevant third parties in order to manage any risks identified by the DPIA or other risk assessment in order to reduce the likelihood of a non-conformance with this policy.

11.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, MVDC shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

11.2.4 Where, as a result of a DPIA it is clear that MVDC is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not MVDC may proceed must be passed for review to the Data Protection Officer.

11.2.5 The Data Protection Officer shall, if there are significant concerns, either as to the potential damage or distress, the quantity of data concerned, or more generally escalate the matter by way of reporting it to the supervisory authority.

Document Owner and Approval

The Data Protection Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on MOLLY.

This policy was approved by MVDC's Executive on *[date]* (with future authority to make amendments delegated to the Data Protection Officer in consultation with the Council's Deputy Chief Executive) and is issued on a version controlled basis under the signature of the Data Protection Officer.

Signature: Date:

Mole Valley District Council

Insert Company Logo

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	<Manager>	Xx/yy/zz

Mole Valley District Council

Insert Company Logo