Civic Centre, Castle Street,
Merthyr Tydfil CF47 8AN

Main Tel: 01685 725000 www.merthyr.gov.uk

Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL
MERTHYR TYDFIL
County Borough Council

FULL COUNCIL REPORT

Date Written	18th July 2016
Report Author	Lisa Richards
Service Area	Legal Services
Exempt/Non Exempt	Non Exempt
Committee Date	28th September 2016

To: Mayor, Ladies and Gentlemen

DATA PROTECTION REFORM – THE GENERAL DATA PROTECTION REGULATIONS (GDPR) 2016

1.0 SUMMARY OF THE REPORT

1.1 The report outlines the changes that the Council will need to implement in order to achieve compliance with the General Data Protection Regulations (GDPR) 2016.

1.2 The Council has until the 25 May 2018 to ensure that we are compliant with the new GDPR.

1.3 The implementation of the GDPR is likely to have significant budgetary, IT, personnel, governance and communications implications for the Council.

1.4 The GDPR places great emphasis on the documentation that the Council must maintain in order to demonstrate accountability. Compliance within all areas listed in this report will require the Council to review our approach to information governance and how we manage data protection as a corporate issue.

1.5 The GDPR requires the Council to appoint a Data Protection Officer who will be responsible for the implementation of the GDPR and data protection compliance across all departments. This post is a statutory requirement as per Article 37 and will contain protected characteristics pursuant to Article 38.

2.0 RECOMMENDATIONS THAT

2.1 The proposals for the implementation of the General Data Protection Regulations be approved.

2.2 The creation of the Data Protection Officer post in accordance with Articles 37-39 of the GDPR be approved and an appointment to the role be made in accordance with Council Policy and Procedures.

2.3 The funding for the Data Protection Officer post is found for 2016/2017 from the Efficiency Reserves and thereafter into the Base Budget.

3.0 INTRODUCTION AND BACKGROUND

3.1 The official title of the new GDPR is REGULATION 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (General Data Protection Regulation).

3.2 The GDPR originated in the European Union (EU) and has been drafted in order to make the United Kingdom fit for the digital age. The GDPR will replace the UK's existing Data Protection Act which was developed in accordance with the 1995 Data Protection Directive (95/46/EC).

3.3 The GDPR is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate the Council's activities by simplifying rules for use in the Digital Single Market.

3.4 On 15 December 2015, the European Parliament, which included representatives from the British Government, reached agreement on the new data protection rules, establishing a modern and harmonised data protection framework across the EU.

3.5 On the 14 April 2016 the GDPR was adopted by the European Parliament. On 4 May 2016, the official texts of the GDPR were published in all the official languages.

3.6 The GDPR entered into force in the UK on 24 May 2016; it shall become enforceable on the Council from 25 May 2018.

3.7 Despite the UK's vote to leave the EU (Brexit), the UK will continue to be a member of the EU in May 2018 and therefore be subject to EU law. In any event the Information Commissioner's Office (ICO) has released a statement explaining that the UK will mirror the GDPR as deviation from these Regulations will deem the UK as an inadequate country for data protection purposes. If we are deemed inadequate then EU member states will not be able to trade within the UK.

3.8 The ICO is the UK's independent public body set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO will monitor organisations to form a view of their performance in adhering to the GDPR.

3.9 The GDPR will impose significant changes on the information governance structure of the Council. This will include how we interact with our clients, the way in which we record information relating to our clients, the way in which we communicate our processing activities to our clients and a number of other areas all relating to the Council's processing activities of personal information. It will have a significant

impact on all directorates and our contractual arrangements with external companies, consultants etc.

4.0 OVERVIEW OF THE PROPOSALS

4.1 The appointment of the Data Protection Officer (DPO):

4.1.1 Article 37 states that all Local Authorities must appoint a Data Protection Officer (DPO). The DPO will initially manage and implement the Data Protection reform therefore ensuring that the Council complies with the GDPR by its implementation date of May 2018. After this date the DPO will have a very specific role in relation to data protection compliance and processing activities across the Council. The main tasks of the DPO are provided within Article 39 however further tasks have been identified by the Council's Information Governance Forum which have been included within the job description.

4.1.2 Article 37 of the GDPR also states that the person who is appointed into the role of the DPO must be designated on the basis of their professional qualities; in particular they will require expert knowledge of data protection law and practices. With this in mind an essential criteria for the post will be that the individual appointed is degree level qualified and holds a BCS/ISEB Certificate in Data Protection and thus qualifying them as a Data Protection Practitioner.

4.1.3 Article 38 provides details relating to the position of the DPO within the Council. This role must report directly to the most senior level of management, therefore ensuring that the role should be treated as a senior position within the Council. The Council's Senior Information Risk Owner, who is also the Deputy Chief Executive, has recognised that the DPO should report directly to him, whilst the Head of Legal and Governance Services should maintain day to day line management of the post.

4.1.4 Article 38 also states that the Council must support the DPO in performing their tasks by providing resources necessary to carry out their tasks and to maintain their expert knowledge. As a result of this a budget for Information Governance will need to be created. All expenditure from this budget has to be authorised by the DPO. Failure to provide an adequate budget would be classed as a breach of the Regulations. Further information relating to the budgetary requirements of the data protection reform has been included within point 5 of this report.

4.1.5 Article 38 also explains that the role of the DPO contains protected characteristics, it outlines that the DPO must be allowed to act independently of the Council and should not receive instructions from their employer on how they are to discharge their statutory functions. The DPO cannot be dismissed or penalised by the Council for performing these tasks.

4.1.6 In accordance with the GDPR the tasks of the DPO cannot be delegated to a junior member of staff, as such the Council must create a new post in order to demonstrate compliance with this Regulation.

4.2 Accountability and Governance:

4.2.1 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. While the principles of accountability and transparency have previously been implicit requirements of data protection law, the GDPR's emphasis elevates their significance. The new accountability principle in Article 5(2) requires the Council to demonstrate that we comply with the principles.

4.2.2 The Council will be expected to put into place comprehensive but proportionate governance measures. Good practice tools such as privacy impact assessments and privacy by design are now legally required in certain circumstances. These will be discussed in further detail under point 4.3 below.

4.2.3 These measures are designed to minimise the risk of data protection breaches and uphold the protection of personal data. Practically, this is likely to mean further guidance for officers is produced, additional policies and procedures will be implemented for the Council and current policies will be updated to ensure they reflect appropriately on these new requirements.

4.2.4 In order to demonstrate compliance with Article 5 the Council must implement appropriate technical and organisational measures that ensure and demonstrate that we comply. This will include the creation of several internal data protection policies, increased staff training, internal audits of processing activities, and reviews of internal HR policies. The Council will be required to maintain relevant documentation on processing activities; this is similar to the current data controller registration process which is administered by the ICO. In addition to registering these details with the ICO the Council will be required to make these records that outline our processing activities available to the relevant supervisory authorities for investigatory purposes.

4.3 Data protection by design and data protection by default:

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Under the GDPR the Council has an obligation to implement technical and organisational measures to prove that the Council has considered and integrated data protection into our processing activities. The Council will be required to ensure that privacy and data protection is a key consideration in the early stages of any project which includes the following:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

4.3.1 Data Protection Impact Assessments:

As per Article 35 a Data Protection Impact Assessment will need to be created in order to identify the most effective way to comply with the data protection obligations and meet individuals' expectations of privacy.

A Data Protection Impact Assessment will outline the description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the Council. It will evaluate the necessity and proportionality of the processing in relation to the purpose. It will assess and establish potential risks to individuals and allow the Council to put measures in place in order to limit any risks by increasing the security of the data thus demonstrating that the Council is complying with the Regulations. The DPO will be responsible for overseeing this process.

4.3.2 Privacy Notices:

The GDPR places an obligation on the Council to provide individuals with fair processing information in the form of a privacy notice. The current data protection provisions require the Council to inform individuals of our processing activities, the GDPR emphasises the need for transparency over how we use personal data.

The GDPR sets out the information that the Council must supply and when individuals should be informed. The information contained within our privacy notices will be determined by whether or not we obtained the personal data directly from individuals.

Much of the information contained within the privacy notice should be consistent with our current obligations under the DPA, but there is further information we are explicitly required to provide, such as:

- The identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer
- Purpose of the processing and the legal basis for the processing
- The legitimate interests of the controller or third party, where applicable
- Categories of personal data
- Any recipient or categories of recipients of the personal data
- Details of transfers to third country and safeguards
- Retention period or criteria used to determine the retention period
- The existence of each of data subject's rights
- The right to withdraw consent at any time, where relevant
- The right to lodge a complaint with a supervisory authority
- The source the personal data originates from and whether it came from publicly accessible sources

- Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data

- The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

The GDPR also requires further information to be placed within our privacy notices about the processing of personal data which must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The Council will be required to redraft our current privacy notices which do not satisfy the conditions set out under Articles 12 and 13 of the GDPR and communicate the updated versions to our clients.

The Council will also need to identify any departments that are currently processing personal information without appropriate privacy notices in place. This process will need to be documented in order to demonstrate compliance with Articles 12 and 13. The DPO will take the lead role in this area.

4.3.3 Records of processing activities:

In order to ensure that the Council can demonstrate that we are complying with the GDPR we must be proactively documenting our processing activities.

This will primarily be set out within our obligation to provide comprehensive, clear and transparent privacy policies however we must also maintain additional internal records of our processing activities. It is therefore essential that the data protection audits are carried out across all departments processing personal data, on an annual basis in order to ensure we are complying and continue to comply with the GDPR.

The DPO will take the lead role in conducting these audits, liaising with the Council's Internal Audit Department when required.

4.4 A change in how we obtain consent:

4.4.1 The GDPR has references to both 'consent' and 'explicit consent'. The difference between the two is not clear given that both forms of consent have to be freely given, specific, informed and an unambiguous indication of the individual's wishes.

4.4.2 Consent under the GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent. Some form of record must be kept of how and when consent was given. Individuals have a right to withdraw consent at any time.

4.4.3 Implementation of the GDPR will require the Council to carry out a review of consent mechanisms to ensure they meet the standards required under the legislation.

4.5 New rights for individuals:

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The GDPR provides the following rights for individuals:

4.5.1 The right to be informed:

The right to be informed encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data. This has been outlined under point 4.3.2 above.

4.5.2 The right of access:

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

The right to access is similar to the existing subject access rights under the DPA. However Article 12 of the GDPR provides for a substantial change as the Council must provide copies of information free of charge. Therefore the GDPR removes the current requirement of the £10 statutory fee.

The time limits for a response have changed. The Council will have less time to comply with a data request under the GDPR. Under Article 14 of the GDPR information must be provided without delay and at the latest within one month of receipt. Currently the Council has 40 calendar days to respond to a request from receipt of the fee. Under the new provisions time limit for compliance will vary depending upon the month it has been received. Please see below for further details:

January = 31 calendar days to respond
February = 28 calendar days to respond (except on a leap year)
March = 31 calendar days to respond
April = 30 calendar days to respond
May = 31 calendar days to respond
June = 30 calendar days to respond
July = 31 calendar days to respond
August = 31 calendar days to respond
September = 30 calendar days to respond
October = 31 calendar days to respond
November = 30 calendar days to respond
December = 31 calendar days to respond

Please note, weekends and bank holidays are included within the timeframes outlined under the GDPR. The removal of the fee and the reduction in time for a response will cause a significant strain on Council resources, particularly within departments that hold and process a vast amount of personal data.

Additionally the Council has only one member of staff that deals with requests of this nature (in addition to a number of other tasks). This is a major change for the Council and should we fail in our responsibilities under Articles 12 and 14 we could face a fine of up to €20 million per article breached. If both articles are breached i.e. the Council imposes a fee or the deadline has been missed, the maximum fine the Council could be subject to is €40 million.

The Council will still be required to verify the identity of the person making the request, using reasonable means. We currently seek one form of photographic ID and proof of address; with regards to children we also require a copy of their long birth certificate. This process will remain unchanged.

Recital 63 introduces a new best practice recommendation that, where possible, the Council should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This will impact the Council's ICT section as they will be required to both design and create a new system or source a suitable system for purchase. If the Council could create an online system within which responses to personal data requests could be uploaded we would save in postage, however staff time would not be reduced as the information would need to be verified before being placed within this domain.

4.5.3 The right to rectification:

Individuals are currently entitled to have personal data rectified if it is inaccurate or incomplete under the DPA. However the GDPR states that if we have disclosed the personal data in question to third parties, we must inform them of the rectification where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

4.5.4 The right to erasure:

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

4.5.5 The right to restrict processing:

Under the DPA, individuals have a right to 'block' or suppress processing of personal data. The restriction of processing under the GDPR is similar.

When processing is restricted, the Council will be able to store the personal data, but we will not be able to further process it. We must retain just enough information about the individual to ensure that the restriction is respected in future.

4.5.6 The right to data portability:

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

This will be useful to the Council where several departments provide services to the same individual or where a service user will transition from Children's Social Services into Adult Social Services.

It will impact the Council's current internal data sharing arrangements, at present the Council must rely upon the exemptions and conditions for processing under the existing DPA, the introduction of this new right removes this burden, the Council will of course be required to keep accurate documentation demonstrating our compliance with the Regulations.

4.5.7 The right to object:

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

This will mean that the Council will have to implement policies and procedures to ensure that where we are processing data for the purposes listed above individuals are given the opportunity to object and there are means for us to withdraw their data if they decide to object.

4.5.8 Rights in relation to automated decision making and profiling:

The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. These rights work in a similar way to existing rights under the DPA.

The Council will need to carry out a review of all our ICT systems in order to identify whether any of our processing operations constitute automated decision making. Once we have established what systems are making automated decisions we will be required to update our procedures to deal with the requirements of the GDPR.

4.6 New rights for children:

4.6.1 The GDPR contains new provisions intended to enhance the protection of children's personal data. Where services are offered directly to a child, the Council must ensure that our privacy notice, and any other documentation we produce relating to these types of processing activities are written in a clear, plain way that a child will understand. If the Council offers an online service to

children, we will need to obtain explicit consent from a parent or guardian to process the child's data. This particular element of the GDPR may impact children's social services or education services. A review of our online presence will need to be carried out to ensure we are compliant with Article 8.

4.6.2 The GDPR states that parental/guardian consent for access to online services is required for children aged 16 and under. In Britain currently we legally have to obtain consent from a parent when a child is 13 and under.

4.6.3 Online Services includes most internet services provided at the user's request and for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles. The Council hosts some schools information within our network, some of the schools access 'Moodle' an education platform where each pupil will have a profile.

4.6.4 Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

4.7 Existing and new contractual arrangements:

4.7.1 The Council will be required to carry out a review of all existing contractual arrangements which involve third parties processing the Council's personal data. This review will identify what contracts will need to be updated and redrafted where appropriate. It is essential that the contracts register has been completed in order for an effective review to take place.

4.7.2 During the 2017-2018 financial year the DPO will be required to future proof all new contractual arrangements within which personal data is going to be processed by any contractors. This will involve the drafting and updating of the data protection clauses that can be found within the body of the contracts. Other agreements, such as database access agreements, data processing agreements, data disclosure agreements and also the information sharing protocols will need to be re-negotiated in order for them to comply with the new regulations.

4.7.3 Ensuring compliance across all contractual agreements will involve significant resources and officer time.

4.8 Breach notification:

4.8.1 The GDPR introduces a legal duty on the Council to report certain types of data breaches to the relevant supervisory authority, the ICO, and in some cases to the individuals affected.

4.8.2 The Council will be required to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

4.8.3 Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must notify those concerned directly. Under the GDPR high risk relates to the threshold for notifying individuals and has to be higher than the risk for notifying the ICO.

4.8.4 A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the Council becoming aware of it. This is a major concern as the majority of breaches are not reported to the relevant officer within this timescale let alone the ICO. Therefore new policies will be implemented relating to breach notifications and potential disciplinary action where there is a failure to follow the policy. The Council must strengthen its current breach notification policies and disseminate this information to all staff.

4.8.5 Staff processing personal data will be required to undertake training relating to what constitutes a data breach, in order to raise awareness of the new obligations imposed by the GDPR. In light of the tight timescales for reporting a breach - it is important for the Council to implement robust breach detection, investigation and internal reporting procedures. The ICO guidance states that organisations should put in place an internal breach reporting procedure so that they can comply with their obligations to notify personal data breaches. It said an internal breach reporting procedure will facilitate decision-making about whether we need to notify the relevant supervisory authority or the public.

4.8.6 In order to assess the risks associated with each breach the Council will need to implement a system which can assess whether a breach is high or low risk, this will help determine whether or not we are required to formally report the breach and whether we should notify the affected individuals.

4.9 <u>Failure to comply with the GDPR:</u>

4.9.1 If the Council fails to notify a breach to the ICO within the 72 hour period or if we fail to comply with any aspect of the GDPR we could be facing significant fines of up to €10 million or 2% of total worldwide annual turnover (whichever is the greatest) for level 1 fines, and fines of up to €20 million or 4% of total worldwide annual turnover (whichever is the greatest) for level 2 fines.

In terms of actions that could result in a level one fine, it could be for an infringement of any one of 19 different Articles which are as follows:

Article 8	Conditions applicable to child's consent in relation to information society services
Article 11	Processing which does not require identification
Article 25	Data protection by design and by default
Article 26	Joint controllers
Article 27	Representatives of controllers or processors not established in the Union
Article 28	Processor
Article 29	Processing under the authority of the controller or processor
Article 30	Records of processing activities
Article 31	Cooperation with the supervisory authority

Article 32	Security of processing
Article 33	Notification of a personal data breach to the supervisory authority
Article 34	Communication of a personal data breach to the data subject
Article 35	Data protection impact assessment
Article 36	Prior consultation
Article 37	Designation of the data protection officer
Article 38	Position of the data protection officer
Article 39	Tasks of the data protection officer
Article 41	Monitoring of approved codes of conduct
Article 42	Certification
Article 43	Certification bodies

Level two fines are for the more serious offences, relating to infringement of 23 further Articles which have been outlined below:

Article 5	Principles relating to personal data processing
Article 6	Lawfulness of processing
Article 7	Conditions for consent
Article 9	Processing of special categories of personal data
Article 12	Transparent information, communication and modalities for the exercise of the rights of the data subject
Article 13	Information to be provided where personal data are collected from the data subject
Article 14	Information to be provided where personal data have not been obtained from the data subject
Article 15	Right of access by the data subject
Article 16	Right to rectification
Article 17	Right to erasure (‘right to be forgotten’)
Article 18	Right to restriction of processing
Article 19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
Article 20	Right to data portability
Article 21	Right to object
Article 22	Automated individual decision-making, including profiling
Article 44	General principle for transfers
Article 45	Transfers on the basis of an adequacy decision
Article 46	Transfers subject to appropriate safeguards
Article 47	Binding corporate rules
Article 48	Transfers or disclosures not authorised by Union law
Article 49	Derogations for specific situations
Article 58	Powers
Article 85	Processing and freedom of expression and information
Article 86	Processing and public access to official documents
Article 87	Processing of the national identification number
Article 88	Processing in the context of employment
Article 89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 90 Obligations of secrecy
Article 91 Existing data protection rules of churches and religious associations

If the Council wishes to avoid enforcement action and any potential fines then the recommendations outlined within this report will need to be approved.

5.0 FINANCIAL IMPLICATION(S)

5.1 The following financial implications are attached to this report:

Information Governance	Estimate 2016-2017	Estimate 2017-2018	Estimate 2018-2019	TOTAL
Expenditure				
Employee Costs				
Salaries				
Data Protection Officer	£25,805	£54,850	£57,840	£138,495
Information Governance Officer	£15,575	£33,410	£35,620	£84,605
Staff Training	£7,040	£950	£950	£8,940
Transport Related Expenditure				
Travelling & Subsistence	£250	£500	£500	£1,250
Supplies & Services				
ICT Equipment	£1,000	£100	£100	£1,200
Office Equipment	£550	£0	£0	£550
Stationery	£200	£200	£200	£600
Meeting/staff training costs	£0	£300	£300	£600
Gross Expenditure	£50,420	£90,310	£95,510	£236,240

Further breakdown of the financial details:

ICT equipment (for 1 member of staff)	
Laptop	£368
Docking station	£66
Screen	£71
Keyboard	£10
Mouse	£5
Office Licence	£213
Phone	£96
Good App	£134
TOTAL	£963

Office Equipment	
Desk*2	£178
Chair*2	£158
Filing cabinet/cupboard	£200
TOTAL	£536

5.2 For 2016/17 the additional funding requirement will be borne by earmarked reserves with future years' commitments built into the Council's Medium Term Financial Plan.

6.0 SINGLE INTEGRATED PLAN AND SUSTAINABILITY IMPACT SUMMARY

6.1 The Single Integrated Plan and Sustainability Impact Assessment has been completed and the proposals have no negative impact on all aspects of the Corporate Plan and Single Integrated Plan. No negative impacts have been identified.

7.0 EQUALITY IMPACT ASSESSMENT

7.1 An Equality Impact Assessment (EqIA) form has been prepared for the purpose of this report. It has been found that a full assessment is not required at this time. The form can be accessed on the Council's website/intranet via the 'Equality Impact Assessment' link.

GARETH CHAPMAN
CHIEF EXECUTIVE

COUNCILLOR PHIL WILLIAMS
CABINET MEMBER FOR GOVERNANCE AND CORPORATE SERVICES

BACKGROUND PAPERS		
Title of Document(s)	**Document(s) Date**	**Document Location**
Data Protection Officer's Job Description	26/07/2016	Legal Services
Tasks of the Data Protection Officer	26/07/2016	Legal Services
Information Governance Team Structure	26/07/2016	Legal Services
Information Governance Officers Job Description	26/07/2016	Legal Services
Tasks of the Information Governance Officer	26/07/2016	Legal Services

Does the report contain any issue that may impact the Council's Constitution?	**No**

Consultation has been undertaken with the Corporate Management Team in respect of each proposal(s) and recommendation(s) set out in this report.