This information is available free of charge in electronic, audio, Braille and large print versions on request.

For assistance in understanding or reading this document or specific information about this Agenda or on the "Public Participation" initiative please call Democratic Services on 01629 761133 or e-mail committee@derbyshiredales.gov.uk

21 February 2018

To: All Councillors

As a Member or Substitute of the **Governance and Resources Committee**, please treat this as your summons to attend a meeting on **Thursday 1 March 2018 at 6.00pm in the Council Chamber, Town Hall, Matlock.**

Yours sincerely

Sandra Lamb
Head of Corporate Services

AGENDA

1. APOLOGIES/SUBSTITUTES

Please advise Democratic Services on 01629 761133 or e-mail committee@derbyshiredales.gov.uk of any apologies for absence and substitute arrangements.

2. APPROVAL OF MINUTES OF PREVIOUS MEETING

18 January 2018

3. PUBLIC PARTICIPATION

To enable members of the public to ask questions, express views or present petitions, **IF NOTICE HAS BEEN GIVEN**, (by telephone, in writing or by electronic mail) **BY NO LATER THAN 12 NOON OF THE WORKING DAY PRECEDING THE MEETING**.

4. INTERESTS

Members are required to declare the existence and nature of any interests they may have in subsequent agenda items in accordance with the District Council's Code of Conduct. Those interests are matters that relate to money or that which can be valued in money, affecting the Member her/his partner, extended family and close friends.

Interests that become apparent at a later stage in the proceedings may be declared at that time.

Published 21 February 2018

5. QUESTIONS PURSUANT TO RULE OF PROCEDURE NUMBER 15.

To answer questions from Members who have given the appropriate notice.

Page No.

6. INTERNAL AUDIT REPORTS CONCLUDED UNDER THE 2017/2018 OPERATIONAL AUDIT PLAN **3 - 6**

To consider the internal audit reports produced in respect of the 2017/2018 Internal Audit Plan.

7. INTERNAL AUDIT OPERATIONAL PLAN 2018/19 **7 - 15**

To consider the Internal Audit Operational Plan 2018/2019 which outlines the assignments and estimated resources needed during the year.

8. DATA PROTECTION **16 - 35**

To note the progress made against the General Data Protection Regulation Action Plan and consider approval of the Data Protection Policy along with delegation of authority to the Head of Resources to make minor amendments to the Policy.

9. REFERRED ITEM – MANAGING VIOLENCE, BULLYING, HARASSMENT AND AGGRESSION AT WORK POLICY **36 - 37**

To consider a recommendation from the Joint Consultative Committee meeting held on 8 February 2018 to adopt the Managing Violence, Bullying, Harassment and Aggression at Work Policy.

10. JOINT CONSULTATIVE GROUP: MINUTES OF 8 FEBRUARY 2018 **38 - 39**

To receive the Minutes of the Joint Consultative Group meeting held on 8 February 2018.

11. EXCLUSION OF PUBLIC AND PRESS

At this point the Committee will consider excluding the public and press from the meeting for the remaining items of business for the reasons shown in italics. The Chairman will adjourn the meeting briefly to enable members of the public to speak to Councillors.

12. ARREARS FOR WRITE OFF – CONFIDENTIAL REPORT **40 - 48**

To consider the write off of debts that has been pursued by all appropriate means of recovery by the Council.

(This report contains information relating to an individual where disclosure may be a breach of the Council's Data Protection Act).

Members of the Committee - Councillors Deborah Botham, Albert Catt, Steve Flitter, Chris Furness (Vice Chairman), Alyson Hill, Neil Horton, Angus Jenkins, Tony Millward BEM, Jean Monks, Garry Purdy, Mike Ratcliffe, Lewis Rose, Mark Salt, Jacquie Stevens (Chairman), Colin Swindell, John Tibenham, Jo Wild

Substitutes – Councillors Jason Atkin, Richard Bright, Jennifer Bower, Sue Bull, Sue Burfoot, David Chapman, Tom Donnelly, Ann Elliott, Helen Froggatt, Susan Hobson, Richard FitzHerbert, Vicky Massey-Bloodworth, Dermot Murphy, Joyce Pawley, Irene Ratcliffe, Philippa Tilbrook

NOT CONFIDENTIAL – For public release Item No. 6

GOVERNANCE AND RESOURCES COMMITTEE
1 MARCH 2018

Report of the Head of Resources

INTERNAL AUDIT REPORTS CONCLUDED UNDER THE 2017/2018 OPERATIONAL AUDIT PLAN

PURPOSE OF REPORT

This report asks the Committee to consider the internal audit reports produced in respect of the 2017/2018 Internal Audit Plan.

RECOMMENDATION

That the Committee note the findings and conclusions of the internal audit reviews that have taken place this period.

WARDS AFFECTED

None

STRATEGIC LINK

Internal Audit's service aims and objectives are the provision of an independent service, which objectively examines, evaluates and reports to the Council and its management on the adequacy of the control environment. This contributes to the Council's core values of being open and transparent when making decisions and using public resources ethically and responsibly.

---

1 SUMMARY

1.1 The 2017/18 Operational Audit Plan was approved by the Governance and Resources Committee on 23 March 2017. It provides a framework by which service functions are reviewed to test and report on the adequacy and effectiveness of risk management systems and the internal control environment within the Council. This report details the results of the internal audit reviews undertaken during the year.

1.2 The Committee's terms of reference also require that it "considers the reports produced in accordance with the Audit Plan and responses to the recommendations made therein".

2 REPORT

2.1 Attached, as Appendix 1, is a summary of reports issued since this committee last considered a report for audits included in the 2017/18 Internal Audit Plan.

2.2 Reports are issued as Drafts with five working days being allowed for the submission of any factual changes, after which time the report is designated as a Final Report. Fifteen working days are allowed for the return of the Implementation Plan.

2.3 The Appendix shows for each report a summary of the level of assurance that can be given in respect of the audit area examined and the number of recommendations made / agreed where a full response has been received.

2.4 The assurance provided column in Appendix 1 gives an overall assessment of the assurance that can be given in terms of the controls in place and the system's ability to meet its objectives and manage risk in accordance with the following classifications:

Assurance Level	Definition
Substantial Assurance	There is a sound system of controls in place, designed to achieve the system objectives. Controls are being consistently applied and risks well managed.
Reasonable Assurance	The majority of controls are in place and operating effectively, although some control improvements are required. The system should achieve its objectives. Risks are generally well managed.
Limited Assurance	Certain important controls are either not in place or not operating effectively. There is a risk that the system may not achieve its objectives. Some key risks were not well managed.
Inadequate Assurance	There are fundamental control weaknesses, leaving the system/service open to material errors or abuse and exposes the Council to significant risk. There is little assurance of achieving the desired objectives.

2.5 Four reports have been issued, all 4 with a conclusion of "substantial Assurance". One low priority and one high priority recommendations have been made and accepted.

3 RISK ASSESSMENT

3.1 Legal

There are no legal considerations arising from the report

3.2 Financial

There are no financial considerations arising from the report.

3.3 Corporate Risk

There are no corporate risks to consider

4 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

5 CONTACT INFORMATION

Karen Henriksen, Head of Resources
Telephone: 01629 761284; Email: karen.henriksen@derbyshiredales.gov.uk

Sandra Lamb, Head of Corporate Services
Telephone: 01629 761281; Email: sandra.lamb@derbyshiredales.gov.uk

Jenny Williams, Internal Audit Consortium Manager
Telephone: 01246 345468; Email: Jenny.williams@chesterield.gov.uk

6 BACKGROUND PAPERS

None

7 ATTACHMENTS

Appendix 1 - Summary of Internal Audit Reports Issued October 2017 – January 2018

Appendix 1

DERBYSHIRE DALES DISTRICT COUNCIL

Internal Audit Consortium - Report to Governance and Resources Committee

Summary of Internal Audit Reports Issued October 17 – January 18

Report Ref	Report Title	Scope and Objectives	Overall Opinion	Date		Number of Recommendations	
				Report Issued	Response Due	Made	Accepted
D007	Housing Benefits	To ensure that benefits are paid promptly and accurately	Substantial	31/10/17	21/11/17	0	0
D008	Council Tax	To ensure that bills are raised promptly and accurately and that there are good collection procedures in place	Substantial	6/12/17	4/01/18	1L	1
D009	Cash and Bank	To review the adequacy of the controls and systems in place in respect of the cash and bank system.	Substantial	3/01/18	24/01/18	0	0
D010	Non Domestic Rates	To ensure that bills are raised promptly and accurately and that there are debt collection procedures in place	Substantial	24/01/2018	14/02/2018	1H	1

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 7

GOVERNANCE AND RESOURCES COMMITTEE
1 MARCH 2018

Report of the Head of Resources

INTERNAL AUDIT OPERATIONAL PLAN 2018/19

PURPOSE OF REPORT

This report asks the Committee to agree the Internal Audit Operational Plan 2018/19 which outlines the assignments and estimated resources needed during the year.

RECOMMENDATIONS

That the internal audit plan for 2018/19 be agreed.

WARDS AFFECTED

None

STRATEGIC LINK

The Audit Plan is linked to the Council's Performance Plan values by reviewing service functions and testing and reporting on service quality and governance provisions. This also fits in with the Council's aim to provide an excellent service.

---

1 SUMMARY

1.1 A key requirement of the Public Sector Internal Audit Standards is that a periodic risk based plan should be prepared that should be sufficiently flexible to reflect the changing risks and priorities of the organisation. The risk based plan should be fixed for a period of no longer than one year, should outline the assignments to be carried out, their respective priorities and the estimated resources needed.

1.2 A note explaining the role, purpose and some of the terminology used in the internal audit plan is attached at Appendix 1.

1.3 An annual report summarising the outcome of the 2017/18 internal audit plan will be presented to this Committee after the year-end.

2 REPORT

2.1 A summary of the internal audit plan for 2018/19 is shown below and the detailed plan is shown as Appendix 2.

Internal Audit Plan 2018/19

Summary	Audit Days
Main Financial Systems	88
Other Operational Audits	40
Computer / IT Related	12
Corporate / Cross Cutting	17
Special Investigations & Contingency	15
Provision of financial advice	10
Management Service	30
Grand Total	**212**

2.2 The plan has been prepared taking into account the following factors:-

- The organisational objectives and priorities
- Local and national issues and risks
- The requirement to produce an annual internal audit opinion
- The organisations assurance framework
- The internal audit risk assessment exercise covering the financial control and other procedures subject to audit
- The Council's Strategic Risk Register
- The views of the Head of Resources

2.3 It is important to note that the audit plan is 212 productive days which is the time of a Senior Auditor at 4 days a week and the provision of a management service by the Internal Audit Consortium Manager. The number of audit days in the plan was reduced when the Apprentice left last year and prior to that when the Chief Internal Auditor retired. As a consequence, the frequency of audits has been reduced. High priority audits are still examined every year however medium priority audits have moved from a 2 year cycle to a 3 year cycle and low priority audits have moved from a 3 to a 5 year cycle. Forward planning has identified that even given this approach, in 2020/21 there will be considerably more days required then are available to achieve the plan at the current frequency levels. This issue is under discussion with the Head of Resources and the Corporate Leadership Team.

2.4 A copy of the audit plan is provided to the Council's External Auditor to assist in co-ordination of work programmes.

2.5 A copy of the three year audit plan covering the period 2017/18 – 2019/20 is attached for information as Appendix 2. The plan for 2019/20 is indicative only and could well change in order to meet the priorities of the Council.

3 RISK ASSESSMENT

3.1 Legal

There are no legal considerations arising from the report.

3.2 Financial

There are no financial considerations arising from the report. No formula exists that can be applied to determine internal audit coverage needs. However, as a guide, the minimum level of coverage is that required to give an annual evidence-based opinion. It is believed that the level of coverage provided by the proposed 2017/18 internal audit plan will be sufficient upon which to base an opinion.

3.3 Corporate Risk

There are no corporate risks to consider

4 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

5 CONTACT INFORMATION

Karen Henriksen, Head of Resources
Telephone: 01629 761284; Email: karen.henriksen@derbyshiredales.gov.uk

Sandra Lamb, Head of Corporate Services
Telephone: 01629 761281; Email: sandra.lamb@derbyshiredales.gov.uk

Jenny Williams, Internal Audit Consortium Manager
Telephone: 01246 345468; Email: Jenny.williams@chesterield.gov.uk

6 BACKGROUND PAPERS

None

7 ATTACHMENTS

Appendix 1 Internal Audit Plan – Background Note
Appendix 2 Draft Internal Audit Plan 2018/19

Appendix 1

INTERNAL AUDIT PLAN

BACKGROUND NOTE

1. Definition of Internal Audit

Internal Audit is defined in the Public Sector Internal Audit Standards as:

'… an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes".

2. The Purpose of Internal Audit

Internal audit is not a substitute for management. It is the purpose of internal audit to assist and support management by appraising the arrangements and procedures established.

There is also a statutory requirement for internal audit in local government contained in the Accounts and Audit Regulations 2015. These regulations require the authority to undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking in to account public sector internal auditing standards and guidance.

3. The Difference Between Internal Audit and External Audit

External audit is completely independent of the authority. The Council's external Auditors are currently KPMG. Much of the external auditors' work is determined by statutory responsibilities. Internal audit's terms of reference are determined and approved by management.

However, there is nevertheless considerable scope for co-operation to avoid duplication of work and to make maximum use of audit resources.

4. The Scope of Internal Audit Work

One of the essential elements for effective internal auditing is that the internal auditor should adequately plan, control and record their work.

To determine priorities and to assist in the direction and control of audit work the internal auditor will prepare a plan based on a risk assessment.

The audit plan includes the following sections: -

- **Main Financial Systems**
  This covers the fundamental accounting and income collection systems of the authority such as payroll, creditor payments, council tax etc. Most of these systems are reviewed on an annual basis due to their importance.

- **Other Operational Audits**
  Audits to be undertaken in Services include areas such as cemeteries and Section 106/ CIL monies.

- **IT Related**
  Topics in this area of the plan include a review of disaster recovery arrangements.

- **Fraud and Corruption**
  Fraud and corruption is considered in every area of the audit plan, a significant number of audits include an anti-fraud element e.g. income audits.

- **Cross Cutting Issues**
  This area of the plan includes audit subjects that cover all Services or are corporate issues examples include, corporate targets and risk management.

5. Delivering the Internal Audit Service

A three year strategic audit plan is compiled based on an internal audit risk assessment of auditable areas. This risk assessment takes into account the following factors:

- Materiality – the amount of funds passing through the system
- Control Environment / vulnerability – assessed level of control based on previous audit findings
- Sensitivity – profile of the system in relation to customer service
- Management concerns – any specific issues relating to the operation of the system e.g. identified from the Council's Risk Register

Using a scoring system, audits are then categorised as High, Medium or Low risk. This ranking is then used to compile the annual audit plan.
The areas of audit work set out in the agreed plan are split into individual audit assignments.

An audit assignment can involve:

- preparation of system notes and a review/analysis of system controls;
- extraction of background information;
- extraction and testing of sample transactions and controls;
- notes of interviews and meetings.

All work undertaken is recorded on detailed working papers. To ensure that all areas have been covered and appropriate conclusions reached, all working papers are independently reviewed.

A report on the findings and recommendations arising from the audit is sent to the appropriate Head of Service and to the Head of Resources (as Client Officer) at the conclusion of the audit. A response to the recommendations is requested within a set time.

A summary of internal audit reports issued is reported periodically to the Governance and Resources Committee and an Annual Report is submitted after the end of the year detailing the outcome of the audits completed.

	DERBYSHIRE DALES DISTRICT COUNCIL				
		Audit Days			Risk Factor
Main Financial Systems	**H,M,L Priority**	**2017/18**	**2018/19**	**2019/20**	
Main Accounting System	M	6	0	6	Unable to produce an accurate set of accounts / reputational risks
Budgetary Control	M	4	0	4	Lack of control over budgets, overspending(Strategic Risk 1)
Payroll	H	15	13	18	Inaccurate or fraudulent payments, ghost employees
Creditor Payments	H	10	10	8	Incorrect/fraudulent payments (Strategic Risk R6)
Debtors	H	10	13	10	Loss of income (Strategic Risk 6)
Treasury Management	H	6	6	0	Misappropriation of funds/ poor investment decisions
Cash and Banking/petty cash/post opening/bank rec	M	6	6	0	Loss of income theft
Council Tax	H	15	10	10	Loss of income / Fraud(Strategic Risk 6)
Non Domestic Rates	H	10	15	10	Loss of income / Fraud(Strategic Risk 6)
Housing / Council Tax Benefit	H	15	15	15	Reputational damage / fraudulent claims(Strategic Risk 6)
Total Main Financial Systems		**97**	**88**	**81**	
Other Operational Audits	**H,M,L Priority**	**2017/18**	**2018/19**	**2019/20**	**Risk Factor**
Asset Management	M			8	Poor value for money from assets, assets not fit for purpose
Bakewell Leisure Centre	M	8			Loss of income
Car Parks Income	H		4		Loss of income, poor contract management (SR6)
Cemeteries	L		8		Reputational Damage
Choice Based Lettings	M			8	Reputational Damage / fraud
E.Health- Miscellaneous Income	L	8			Loss of income / theft

Other Operational Audits	H,M,L Priority	2017/18	2018/19	2019/21	Risk Factor
Homelessness/Housing Strategy	M	4			Reputational damage
Illuminations	H	2	2	2	Loss of income / fraud
Insurance	M		8		Inappropriate cover / fraud
Leisure Contract Management	H		6	7	Poor contract management arrangements (Strategic Risk 6)
Public Conveniences	L		2		Loss of income / theft
Members Expenses/civic account	L			6	Incorrect payments / fraudulent claims
Section 106/CIL	M		10		Loss of income/reputational damage/ fraud
Taxi Licences/Other Licences	M	8			Loss of income / Safeguarding issues (SR8)
Transport/Plant/Vehicles/Fuel	M	9			Poor fleet management, theft
VAT	M			6	Financial errors
Total Other Operational Audits		**39**	**40**	**37**	
Corporate/Cross Cutting	**H,M,L Priority**	**2017/18**	**2018/19**	**2019/20**	**Risk Factor**
Corporate Targets	M			4	Poor Governance, decisions could be made on incorrect data
Follow up Previous Recommendations	H	5	5	5	Weaknesses continue
Health and Safety	M			10	Reputational Issues/ injury or death, financial cost (SR7)
Procurement	M		8	10	Poor value for money, Fraud (SR4)
Risk Management	M		4		No identification or mitigation of risks
Total Corporate/Cross Cutting		**5**	**17**	**29**	
IT Systems	**H,M,L Priority**	**2017/18**	**2018/19**	**2019/20**	**Risk Factor**
Disaster Recovery	M		8		Failure of key systems/ reputational damage (SR3)
System Security	H	10			Confidential data not secure (SR3)
Cyber Security / Network Security	H		4	8	Failure of key systems/ reputational damage (SR13)
Total IT Systems		**10**	**12**	**8**	

	H,M,L Priority	**2017/18**	**2018/19**	**2019/20**	**Risk Factor**
Fraud and Corruption					
Gifts and Hospitality	L			2	Bribery and corruption
National Fraud Initiative	M	2			Fraud
Total Fraud and Corruption		**2**	**0**	**2**	
Non Audit Duties	**H,M,L Priority**	**2017/18**	**2018/19**	**2018/19**	**Risk Factor**
Elections – Postal Votes	N/A	4	0	0	-
Total Non-Audit Duties		**4**	**0**	**0**	
Other					
Contingency	N/A	10	15	15	
Final Accounts	M	5	0	0	Incorrect payments/ fraud
Financial Advice/Working Groups	H	10	10	10	
Total Other		**25**	**25**	**25**	
Management Time (IA Consortium Manager)	N/A	**30**	**30**	**30**	Non Compliance with PSIAS
Grand Total		**212**	**212**	**212**	

BACK TO AGENDA

NOT CONFIDENTIAL – For public release Item No. 8

GOVERNANCE AND RESOURCES COMMITTEE
1 MARCH 2018

Report of the Head of Resources

DATA PROTECTION

PURPOSE OF REPORT

This report provides an update of progress against the General Data Protection Regulation (GDPR) Action Plan and asks the Committee to approve a Data Protection Policy.

RECOMMENDATIONS

1. That progress against the General Data Protection Regulation (GDPR) Action Plan is noted.
2. That the Data Protection Policy is approved.
3. That delegated authority be given to the Head of Resources to make minor amendments to the Data Protection Policy.

WARDS AFFECTED

None

STRATEGIC LINK

Sound arrangements for information governance and data protection support the District Council's values to be open and transparent when making decisions and to use public resources ethically and responsibly.

---

1 BACKGROUND

1.1 Members will be aware from previous reports to this Committee that the General Data Protection Regulation (GDPR) comes into force in May 2018. The GDPR gives the Information Commissioner's Office (ICO) the power to issue fines of up to €20m, or 4% of turnover, whichever is greater. This demonstrates that the importance of managing Data Protection risk appropriately has increased considerably.

1.2 Members have previously approved a GDPR Action Plan that is aimed at ensuring that the Council will be fully prepared for the introduction of GDPR in May 2018. As this is the last meeting of this Committee before the GDPR comes into force in May, it is considered appropriate to report on progress against the GDPR Action Plan.

2 REPORT

2.1 Progress against GDPR Action Plan

In January 2017, members approved the GDPR Action Plan. Good progress has been achieved in relation to ensuring improved compliance with current legislation and being fully prepared for the changes in May 2018. An updated Action Plan is shown in Appendix 1.

2.2 The GDPR Action Plan includes an action to produce a Data Protection Policy. A draft policy is set out in Appendix 2 for Members' consideration and approval. The policy has been produced to ensure compliance with the relevant legislation and to ensure customers gain appropriate access to data and information on request.

2.3 The Data Protection Policy is written as a mitigation tool should anybody complain or challenge the council. It will provide important evidence for the ICO should a breach occur. It uses the language from the Act and from ICO guidance so that definitions can be understood by third parties such as the ICO and organisations who process data on behalf of the Council.

2.4 The draft Policy has been reviewed by the Corporate Leadership Team and the Council's Information Governance Board.

2.5 The Data Protection Policy will need to be reviewed within a year as the Information Commissioner's Office starts to define the regulations. This is the best that can be produced based on what we know so far.

2.6 Given the pace of change in the GDPR and guidance as the May deadline draws closer, it is recommended that delegated powers be given to the Head of Resources to make minor amendments to the Data Protection Policy.

3 RISK ASSESSMENT

3.1 Legal

Currently, all organisations in the UK that collect, process or store personal information must comply with the Data Protection Act 1998 (DPA), or face fines of up to £500,000 in the event of a data breach.

The Data Protection Act 1998 will soon be replaced by the Data Protection Act 2018, which will bring the provisions of the EU General Data Protection Regulation (GDPR) into UK Law, The GDPR prescribes considerably greater penalties – up to 4% of annual global turnover or €20 million. All organisations that process EU residents' data must comply with the GDPR by 25 May 2018.

The legal risk is therefore currently high with the measure outlined in the report aimed at mitigating that risk to low/medium.

3.2 Financial

The current revenue budget includes provision for the salary and oncosts of an Information Governance Officer, on an ongoing basis. The budget also includes

£50,000 for the cost of an interim resource to manage the implementation of the GDPR Action Plan.

Failure to comply with the Data Protection Act can result in significant fines and/or enforcement action.

The financial risk of implementing the recommendations of this report is assessed as "low".

3.3 Corporate Risk

The Council holds significant amounts of information / data, some of which is classed as personal information. The Council has a responsibility to adopt arrangements that protect personal information while at the same time it faces intense pressure to deliver unprecedented funding cuts, organisational change and innovation in service delivery while meeting public demands for greater transparency in decision-making and performance.

With the Council's aspiration to become paperless, along with mobile and home working arrangements, there is an increased risk that data is shared inappropriately with the wrong individuals/bodies/committees etc. and that information is not appropriately safeguarded. Effective arrangements for data protection will ensure that the Council does not risk financial or reputation damage arising from data protection security breaches

4 OTHER CONSIDERATIONS

In preparing this report, the relevance of the following factors has also been considered: prevention of crime and disorder, equalities, environmental, climate change, health, human rights, personnel and property.

5 CONTACT INFORMATION

Karen Henriksen, Head of Resources

Telephone: 01629 761284; Email: karen.henriksen@derbyshiredales.gov.uk

6 BACKGROUND PAPERS

None

7 ATTACHMENTS

Appendix 1 - General Data Protection Regulation (GDPR) Action Plan

Appendix 2 – Data Protection Policy

Appendix 1

Derbyshire Dales District Council - General Data Protection Regulation (GDPR) Action Plan

Progress as at 16 February 2018

	Actions Completed
	Actions in Progress/Ongoing
	Target date is in the future
	Actions outstanding

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
1	Ensure all office based employees undertake LOLA Data Protection Awareness on-line learning	Human Resources	~~July 2017~~ ~~December 2017~~ February 2018	All employees trained on basic data protection and training records updated.		Completed by majority of office based staff. Reminders sent to those who need to complete the training.	In progress
2	Non office-based employees briefed on data protection.	Data Protection Consultant with managers	~~January 2018~~ February 2018	All employees trained on basic data protection and training records updated.		IGO and DPC to provide training sessions for none office based staff.	Training to be undertaken in March to coincide with GDPR workshops.
3	Plan and deliver a 'Tidy Up Your Data' week'	Data Protection Consultant/ Comms	12th-16th June 2017	Dedicated week of activities, training, surgeries and internal communication	Communicated via SIDD. Links to documents, ICT tip of the day, training delivered etc.		Completed

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
4	Deliver training in the form of a workshop to key staff on data protection Privacy Impact Assessments.	Data Protection Consultant/ Comms	June 2017	Managers aware of the need to build privacy into new service delivery and systems.	Two sessions delivered. 18 officers attended the workshops. Follow on discussions as a result of the training.		Completed
5	Launch documentation on Privacy Impact Assessments following the training.	Data Protection Consultant	June 2017	Managers equipped with the correct paperwork to undertake PIAs	Documentation launched during the training and now available on X drive.		Completed
6	Review 'Data Protection Asset Register' format and add new EU regulation requirements.	Data Protection Consultant	By late April 2017	Accurate central record of information held by each council which is covered by General Data Protection Regulation.	Completed and in use. A check will be needed in 2018 when Regulations are finalised.		Completed
7	With departments, review content of the 'Data Protection Asset Register' and issue action plans for each department/section as appropriate.	Data Protection Consultant/ Information Governance Officer	31 March 2018	Accurate central record of personal data held across the Council.	As at 16/02/18 41 PDARs have been completed and action plans issued as appropriate.		Any newly discovered asset registers will be completed as & when they are discovered.

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
8	Identify all areas of emerging technology to ensure compliance with basic data protection principles.	Data Protection Consultant	June 2017	Links to action above	Guidance given on CCTV to Leisure and Community Safety. Survey Monkey checks done. Leisure on-line checks done.		Completed
9	Data Loss Prevention tool procured to prevent data leakage.	ICT Manager	TBC	Improved email security.	IGB 05/07/17 Agreed that not cost effective		Completed, but agreed not to implement
10	Check X and Y drives to ensure all files containing personal data are locked down.	Data Protection Consultant the Information Governance Officer	June 2017 Then ongoing	No personal data found in insecure areas.	X and Y drive checks completed, with feedback to relevant officers and recommended actions. Will need to be ongoing.	Completed June 2017: Now ongoing	Completed-Now Ongoing
11	Deliver briefing sessions on the implications of the new General Data Protection Regulation to all key managers.	Data Protection Consultant	February 2018	All key managers aware of the changes and the implications for their areas.	9 Sessions have been identified and booked for February		Ongoing
12	'Know Your GDPR' 10 weeks and counting…. Internal publicity on SIDD.	Information Governance Officer/ Comms	~~8th - 12th January 2018~~ 12th -16th March 2018	General internal awareness campaign.		Started "100 days and counting"	Ongoing

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
13	Produce new Data Protection Policy to be approved by CLT and Members	Data Protection Consultant	May 2018	New policy which mirrors duties in General Data Protection Regulation.		Policy has been drafted, reviewed by CLT & the IGB and is awaiting approval by Governance & Resources Committee	
14	Review current Fair Obtaining Notice guidance and prepare Privacy Notice guidelines, include reviewing 'consent'.	Data Protection Consultant	May 2018	Revised guidance for those collecting personal data. Generic Council Privacy Notice. Departments to have reviewed and amended forms, verbal scripts etc. Consent fully covered on Privacy Notices.		Overarching privacy notice has been drafted. Amendments to be made following feedback. Guidance on short privacy notices & consent has also been drafted.	
15	Produce briefing for departments on new 'erasure' requirement.	Data Protection Consultant	May 2018	All departments aware of and able to erase records (if legal) on request.		Ongoing – Been discussed within Personal Data Asset Register (PDAR) reviews.	
16	Consider how personal data will be supplied under new 'data portability' requirement if relevant.	Data Protection Consultant	May 2018	Subject access requests provided electronically.		Ongoing – Been discussed within PDAR. Unlikely that this will be a key issue for Local Government.	

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
17	Update subject access request (SAR) information and procedures.	Data Protection Consultant/ Information Governance Officer	May 2018	Compliant with new regulation from go live date.		To be started and completed before GDPR implementation. Also in consideration for data processors such as Arvato and the Data Protection Protocol.	
18	Establish a procedure for releasing data to third parties (not covered by Information Sharing Agreements) e.g. Police, Inland Revenue, insurance companies etc.	Data Protection Consultant	May 2018	Established process which may need amending once GDPR is in place.		To be started and completed before GDPR implementation.	
19	Rewrite Data Protection Breach Management Guidance into a procedure approved by CLT.	Data Protection Consultant/ Information Governance Officer	May 2018	Formal procedure in place for all employees to work to.		To be started and completed before GDPR implementation	.
20	Consider implications for controller-processor relationship and rewrite Data Sharing Agreements with partners such as Arvato, Serco etc. and review procedures for sharing	Data Protection Consultant/ Information Governance Officer	May 2018	'Data Processor' relationship with Arvato and others re-defined under new regulations.	Some work with Arvato started. PDAR completed with Arvato and Action Plan in place.	Ongoing Monthly meetings scheduled with Arvato & Legal Locum employed to work on contracts	.

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
21	Retention checks should be conducted to ensure data is not being kept longer than is necessary	Information Governance Officer	May 2018	Personal data not being stored electronically or hard copy longer than is necessary.	Some checks undertaken as part of X drive checks and PDAR.	Being addressed PDAR, document to be updated by IGO.	Ongoing
22	Update intranet and website to reflect GDPR.	Information Governance Officer/ Comms	May 2018	Staff and public fully aware of data subject rights.			
23	Review CCTV guidance, control documents etc	Data Protection Consultant	May 2018	Procedures in-line with new regulations.	Some interim documents provided to Leisure and Community Safety.	Community safety provided with documents. System to be review by DPC once privacy zones are in place	.
24	Establishing monitoring procedures to ensure compliance	Information Governance Office /Data Protection Consultant	May 2018	Establish regular reports and PIs as appropriate			
25	Check LOLA (e-learning) for new modular on GPPR, replace existing package and ensure delivered to all office based employees.	Human Resources	July 2018	Mandatory training delivered to employees on new legislation.	LOLA GDPR module checked and it is not appropriate for local government.	In discussions with HR as to possible alternatives. Learning Pool state they are developing a more Local Government appropriate model due for release in February 2018.	

	Action	Who	By When	Expected Outcome	Actual Outcome	Comments	Status?
26	GDPR training workshops to be provide to elected members and senior council officers	Data Protection Consultant/ Information Governance Officer	May 2018	All managers and elected members are aware of the impact of the new legislation and the effect on their service areas.		Officer training due to be completed in February. Looking to arrange elected members Training sessions in May.	
27	Consider implications for Elected Members	Data Protection Consultant/ Information Governance Officer	May 2018	Elected Members compliant with the new regulations		Date dependent on guidance issued	
28	Consider implications for Electoral Registration	Head of Corporate Resources/ Data Protection Consultant/ Information Governance Officer	May 2018	In line with new regulations		Date dependent on guidance issued	
29	Ensuring return of PDAR action plans.	Information Governance Officer	May 2018	In line with new regulations.		Recently chased by IGO with heads of service copied in.	

Appendix 2

DRAFT Data Protection Policy

CONTENTS

		Page No
1.	POLICY	1
2.	SCOPE	1
3.	POLICY PRINCIPLES	2
4.	DATA PROTECTION STATEMENT	2
5.	DATA PROTECTION PRINCIPLES	3
6.	DATA PROTECTION COMPLIANCE	3
7.	DATA SUBJECT'S RIGHTS	5
8.	ACCOUNTABILITY AND GOVERNANCE	6
9.	RESPONSIBILITY FOR IMPLEMENTATION	6

APPENDIX

1	PROCESSING CONDITIONS	7

To be Approved at Governance & Resources Committee 1ST March 2018

DATA PROTECTION POLICY

1. POLICY

1.1. The processing of personal data is essential to many of the services and functions carried out by local authorities. Derbyshire Dales District Council ('the Council') recognises that compliance with the Data Protection legislation will ensure that processing is carried out fairly and lawfully.

1.2. The Data Protection Act, and Article 8 of the Human Rights Act 1998, both stress that the processing of personal data needs to strike a balance between the needs of the organisation to function effectively and efficiently, and respect for the rights and freedoms of the individual. This policy sets out how the Council intends to safeguard those rights and freedoms.

1.3. The Data Protection Act 1998 will be replaced by a revised Act in 2018. The new legislation will build on existing legislation and incorporate the new General Data Protection Regulation, which will be implemented across Europe. Derbyshire Dales District Council recognises the need to abide by the new legislation and associated guidance issued by the Information Commissioner's Office.

1.4. This policy replaces any previous data protection policy statement.

2. SCOPE

2.1 The policy is applicable to all employees, Elected Members, apprentices, agency workers, unpaid volunteers and those on work experience. In certain circumstances it will apply to contractors working for the Council.

2.2 This policy applies to the collection and processing of all personal data as defined by the legislation as that of a 'natural person'. It covers all formats including paper, electronic, audio and visual formats. The policy will only deal with the personal data of a living person and does not apply to the data of a deceased person.

2.3 The policy applies to all employees working within Elections although the post of Electoral Registration Officer is registered, for the processing of elections data, with the Information Commissioners Office separately.

2.4 Key delivery partners who process data on our behalf, such as Arvato Public Services, will have their own policy statements in respect to data protection. These, however, will be in line with the Council's policy.

3. POLICY PRINCIPLES

3.1 The policy is a statement of what the Council is doing to ensure compliance with the legislation. It is not a statement of how compliance will be achieved as this will be a matter for operational procedures.

3.2 The policy has been produced to ensure compliance with the relevant legislation and to ensure customers gain appropriate access to data and information on request. As such the policy will be made available to the public

4. DATA PROTECTION STATEMENT

4.1 The Data Protection Act applies to the processing of personal data wholly or partly by automated means as well as that in filing systems or intended to form part of a filing system at a later date. To be applicable the data has to be stored in a structured way to enable retrieval. '**Filing system**' means any structured set of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis.

4.2 '**Personal data'** means any information relating to an identified or identifiable natural person (data subject). As defined by the legislation an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, a number, location data etc. This may also include online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or radio frequency identification tags. Such identifiers may leave traces which combined with other information may be used to create profiles of the natural person and identify them.

4.2 Derbyshire Dales District Council is the **'Controller'** who determines the purposes and means of processing personal data. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.3 The new legislation applies to **'Processors'** who act on the controller's behalf and places further obligations on both parties. The 'Processor' means a natural or legal person, public body, agency or other body which processes personal data on behalf of the Council. Any processing of personal data in the context of the activities of an establishment of a controller or a processor shall be carried out in accordance with the legislation.

5. DATA PROTECTION PRINCIPLES

5.1. The following **principles** relate to the processing of personal data and set out the main responsibilities for the Council under the legislation. Article 5 of the legislation requires that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject. This will commonly be known as – **lawfulness, fairness and transparency.**

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes. This will be commonly known as – **purpose limitation**.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. This will be commonly known as – **data minimisation.**

(d) Accurate and where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay**.** This will be commonly known as – **accuracy**.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this legislation in order to safeguard the rights and freedoms of the data subject. This will be commonly known as – **storage limitation**.

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. This will be commonly known as – **integrity and confidentiality.**

6. DATA PROTECTION COMPLIANCE

6.1. In order for processing to be lawful the Council must meet one or more conditions, not all of which apply to local government. The conditions for **lawful processing** are detailed in Appendix 1. In general terms the Council will rely on the conditions of ‘legal obligation’ or ‘public task’ as the basis of processing for statutory services and ‘performance of a contract’ for services which are discretionary and allow customer choice.

There will however be circumstances where personal data is highly sensitive and **consent** may form an additional legal basis for processing.

6.2 The Council will explain the reasons for processing personal data through the use of **Privacy Notices. D**epending on the method of contact these may be written as part of a data capture form or verbal. Further details can be found on the Council website.

6.3 In order to deliver services the Council has been regularly processing 'sensitive personal data' such as that relating to the health of an individual or ethnic origin. The new legislation has amended the original list and renamed these **Special Categories**. Personal data which, by their nature, which are particularly sensitive merit specific protection as the context of their processing could create significant risks to the data subject. These are also detailed in Appendix 1.

6.4 The Council has a duty to retain personal data whilst it is legally required to do so. **Security measures** are in place to ensure data is safely stored both in electronic and paper format. The Council has an Information Security Policy to ensure that all staff are aware of their responsibilities. Personal data will be retained in line with the Councils Guidelines on Retention and Disposal of Data, a copy of which is available on request. When data is no longer required it will be safely destroyed or deleted from electronic equipment.

6.4 In order to provide an effective public service the Council may need to share data with third parties and delivery partners who process data on our behalf. Any **sharing of data** will be in line with legislation and where applicable data subjects will be notified as part of the privacy notice. Under certain circumstances where legislation applies the Council will share data with other bodies without consent, for instance for data matching or to prevent fraud or detect crime. A number of Information Sharing Agreements are also in place to ensure effective transfer of data to other bodies, such as the County Council for emergency planning situations and child protection. Such sharing agreements have also been put in place with certain government departments.

6.5 The Council has a duty to ensure that all employees that come into contact with personal data have been adequately trained. This will involve **training** as part of the induction process and throughout the course of their employment. All employees will receive basic data protection and information security training which will be in proportion to the job role undertaken. Refresher training will be mandatory every 2 years for office based employees. Additional on-the-job training may also be necessary in areas processing sensitive or high risk data, such as those containing Special Categories, financial data or using high risk technology. With the assistance of the Data Protection Officer, Human Resources will maintain an accurate record of all data protection training undertaken. Apprentices, unpaid volunteers and those on work experience will receive basic information on the importance of data protection in line with their job role. Elected members will receive regular training on data protection and information security. Delivery partners

who process data on our behalf will also have to demonstrate that they train their employees.

6.6 As stated the Council will ensure measures are in place to protect data, however data breaches may occur. A **data breach** is defined as a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Council will investigate all data breaches and establish the risk to individuals such as discrimination, damage to reputation, financial loss, loss of confidentiality or other significant economic or social disadvantage. The Council will maintain a register of data protection breaches and near misses. Where a risk is likely to have a significant detrimental impact the Council will notify the Information Commissioners Office within 72 hours of identification. Under such circumstances the Council also has a duty to notify those concerned directly. If a breach occurs, the Council and where appropriate its delivery partners, will decide the most appropriate method of communication. This may include placing messages on the website, sending letters or notifying the data subject by telephone. Any breaches reported to the Information Commissioners Office will be done so in accordance with their guidance.

7. DATA SUBJECT'S RIGHTS

7.1. The Council will have operational processes in place to ensure the following data subject's rights apply:

a. The right to be informed
b. The right of access
c. The right of rectification
d. The right of erasure
e. The right to restrict processing
f. The right of data portability
g. The right to object
h. Rights in relation to automated decision making and profiling.

7.2. Under the legislation individuals have a right to obtain confirmation that their data is being processed, have access to their personal data and be provided with other supplementary information on how their data is being used through the use of a privacy notice. The request for access will commonly be done through a Subject Access Request.

7.3 The identity of the individual making the Subject Access Request must be verified using two forms of formal identification which includes both the name and address. This is to ensure that the Council only releases information to the correct data subject. This verification could be a bank statement, passport, utility bill, driving license etc. If visual information is being requested e.g. CCTV images, photographic identification of the data subject will also be needed. If Officers have any reasonable doubt about the identity of an individual they have a right to refuse the request. The Council will take every care to redact any information on other data subjects within the documents before release.

7.4 The personal data requested will be provided **free of charge**. A 'reasonable fee' (based on administrative cost) can be charged if a

request is manifestly unfounded or excessive in nature, or repetitive. In such circumstances a refusal notice will be issued without undue delay and at the latest within one month. The legislation permits the Council to seek clarification from the requestor if necessary.

7.5 The Council will have **one month** from receipt of request to provide the information, ideally however the information will be provided without delay. Complex requests can be extended for a further 2 months, although the requester will be informed within the original one month period. The Council has an operational procedure in place to deal with subject access requests. Information for members of the public wishing to make a Data Subject Access Request can be found on the website. Employees wishing to make a Data Subject Access Request for access to their own personal data should contact Human Resources.

7.6 The Council will have in place operational procedures for the additional rights of rectification, erasure, restricting processing, data portability, objection and rights in respect to automated decision making/profiling. Some of these rights will depend on the original condition for processing and may not apply.

7.7 Should any member of the public wish to make a complaint about the processing of their data by the Council then they should use the Councils Complaints Procedure which is available on the website. The public also have a right to contact the Information Commissioners Office who are the supervisory authority for data protection matters under the legislation.

8. ACCOUNTABILITY AND GOVERNANCE

8.1 The Council will implement appropriate technical and organisational measures to ensure that they are compliant with the legislation and have good governance arrangements in place. The Council will:

- Maintain relevant documentation on processing activities.
- Have a designated Data Protection Officer at an appropriate level within the organisation and provide suitable resources to support the role.
- Implement measures to meet the principle of data protection by design and default, through the use of Data Protection Impact Assessments.
- Ensure transparency and pseudonymisation of data where appropriate.
- Create and improve security measures on an on-going basis.

8.2. The Council has an Information Governance Board which monitors and implements data protection compliance. Reports are also taken to senior management and to elected members. Internal Audit periodically conduct checks on data protection compliance. External inspection and support has also been sought on compliance issues to ensure effective implementation of the legislation.

9. RESPONSIBILITY FOR IMPLEMENTATION

9.1 Keeping the policy under review and updating the policy is the responsibility of the Data Protection Officer for the Council. Corporate Leadership Team are responsible for implementing this policy and the legislation in general.

9.2 Managers at all levels are responsible for ensuring that employees, agency workers, apprentices, unpaid volunteers and work placements for whom they are responsible are aware of and adhere to this policy. Managers are also responsible for ensuring that employees are updated in regard to any changes in this policy and receive regular training.

9.3 All Employees need to be aware that a breach of the legislation could result in disciplinary action being taken.

Processing of personal data by the Council will only be lawful if at least **one** of the following applies:

(a) the data subject has given **consent** to the processing of their personal data for one or more specific purposes;
(b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a **legal obligation** to which the controller is subject;
(d) processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
(e) 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 controller;

Within the Act is a further condition as follows:

(f) processing is necessary for the purposes of **legitimate interests** pursued by the controller or by a third party, except where such interest are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

However the guidance states that this will not apply to processing carried out by public authorities in the performance of their tasks. As such this should not be relied upon for processing.

Additional conditions apply to the processing of **Special Category** data that would reveal:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership

and the processing of:

- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation.

Processing of the above are prohibited unless one of the following applies:

(a) the data subject has given **explicit consent** to the processing for one or more specified purposes;

(b) processing is necessary for the purpose of carrying out an obligation such as employment and social security and social protection law;

(c) processing is necessary to protect the vital interests of the data subject and the natural person is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities of a foundation, association or not-for-profit organisation

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems and services;

(i) processing is necessary for reasons of public interest in the area of public health, such as cross border threats to health;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research.

BACK TO AGENDA

February 2018

NOT CONFIDENTIAL – For public release **Item No. 9**

GOVERNANCE & RESOURCES COMMITTEE

1 MARCH 2018

Report of the Chief Executive

REFERRED ITEM

SUMMARY

To consider a recommendation from the Joint Consultative Group meeting held on 8 February 2018 that the Managing Violence, Bullying, Harassment and Aggression at Work Policy be adopted.

RECOMMENDATION

That the Managing Violence, Bullying, Harassment and Aggression at Work Policy be adopted.

WARDS AFFECTED

None

STRATEGIC LINK

The proposed new policy supports the District Council's corporate values of valuing our employees and in being open and transparent when making decisions and will use public resources ethically and responsibly.

REPORT

The relevant minute of the Joint Consultative Committee is reproduced in full, below, to assist Members' understanding of the issues involved, with the recommendation to be approved marked by an arrow (➔). The Policy has been reviewed and amended as requested by the Joint Consultative Group.

MANAGING, VIOLENCE, BULLYING, HARASSMENT AND AGGRESSION AT WORK POLICY

In 2017 the Safety Committee reviewed lone working arrangements and it was agreed that the Harassment and Aggression Policy should be updated. The initial draft was edited by the Human Resources Manager and discussed at the Employee Group meeting on 20 September 2017. Following this meeting the draft policy was sent out for consultation to all staff concluding with discussion at the Employee Group meeting on 13 December 2017 when all comments were incorporated. The proposed policy was then discussed at the Corporate Leadership Team meeting on 16 January 2018 and their comments, together with those of the Data Protection Officer, were incorporated.

Implementation of the new policy will be supported by staff briefings and training for officers most likely to be at risk as identified by the Human Resources Manager in conjunction with Heads of Service.

Following discussion at the meeting it was agreed that Section 9.5.3 was potentially misleading as it infers that only the Council refer an incident of inappropriate behaviour towards an employee from a member of public to the police. Individuals also have the right and it was agreed the section should be reviewed and possibly expanded to reflect this.

It was moved by Councillor Furness, seconded by Councillor Jean Monks and

AGREED (Unanimously) (➔) That subject to a review of Section 9.5.3, the Governance & Resources Committee be recommended to adopt the Managing Violence, Bullying, Harassment and Aggression at Work Policy at its meeting on 1 March 2018.

BACK TO AGENDA

This information is available free of charge in electronic, audio, Braille and large print versions, and in other languages on request.

For assistance in understanding or reading this document or specific information about these Minutes please call the Democratic Services on 01629 761133 or e-mail committee@derbyshiredales.gov.uk

JOINT CONSULTATIVE GROUP

Minutes of a Meeting held on Thursday 8 February 2018 in the Council Chamber, Town Hall, Matlock at 2.30pm

PRESENT Ashley Watts In the Chair

Councillors Tom Donnelly, Stephen Flitter, Chris Furness, Jean Monks, Joyce Pawley and Garry Purdy

Representing UNISON –Keith Postlethwaite and
Representing GMB – Ian Buxton

Dorcas Bunton (Chief Executive), Chrissie Symons (Human Resources Officer), Annette Reading (Democratic & Electoral Services Assistant) and James Riggott Collins (Corporate Support Apprentice)

APOLOGIES

Apologies for absence were received from Councillor Albert Catt, Councillor Lewis Rose, Andy Cairns (UNISON), Jon Bradbury (GMB), Denise Dawson (UNISON) and Deborah Unwin (Human Resources Manager). Councillors Tom Donnelly and Chris Furness attended as nominated substitute members.

MINUTES

It was moved by Councillor Jean Monks, seconded by Councillor Joyce Pawley and

AGREED (Unanimously) That the minutes of the meeting of the Joint Consultative Group held on 20 June 2017 be approved as a correct record.

MANAGING, VIOLENCE, BULLYING, HARASSMENT AND AGGRESSION AT WORK POLICY

In 2017 the Safety Committee reviewed lone working arrangements and it was agreed that the Harassment and Aggression Policy should be updated. The initial draft was edited by the Human Resources Manager and discussed at the Employee Group meeting on 20 September 2017. Following this meeting the draft policy was sent out for consultation to all staff concluding with discussion at the Employee Group meeting on 13 December 2017 when all comments were incorporated. The proposed policy was then discussed at the Corporate Leadership Team meeting on 16 January 2018 and their comments, together with those of the Data Protection Officer, were incorporated.

Implementation of the new policy will be supported by staff briefings and training for officers most likely to be at risk, as identified by the Human Resources Manager in conjunction with Heads of Service.

Following discussion at the meeting it was agreed that Section 9.5.3 was potentially misleading as it infers that only the Council refer an incident of inappropriate behaviour towards an employee from a member of public to the police. Individuals also have the right and it was agreed the section should be reviewed and possibly expanded to reflect this.

It was moved by Councillor Furness, seconded by Councillor Jean Monks and

AGREED (Unanimously) That subject to a review of Section 9.5.3, the Governance & Resources Committee be recommended to adopt the Managing Violence, Bullying, Harassment and Aggression at Work Policy at its meeting on 1 March 2018.

EMPLOYEE GROUP – NOTES OF THE MEETINGS HELD ON 21 JUNE, 20 SEPTEMBER AND 13 DECEMBER 2017

It was moved by Councillor Joyce Pawley seconded by Councillor Chris Furness and

AGREED (Unanimously) That the notes of the Employee Group meetings held on 21 June, 20 September and 13 December 2017 be received.

SAFETY COMMITTEE – NOTES OF MEETINGS HELD ON 9 AUGUST, 18 OCTOBER 2017 AND 30 JANUARY 2018

It was moved by Councillor Joyce Pawley, seconded by Councillor Tom Donnelly and

AGREED (Unanimously) That the notes of the Safety Committee meetings held on 9 August, 18 October 2017 and 30 January 2018 be received.

Meeting Closed 2.45 pm

Chairman

BACK TO AGENDA