Dr J Ives
Chief Executive
South Derbyshire District Council,
Civic Offices, Civic Way,
Swadlincote, Derbyshire DE11 0AH.

www.southderbyshire.gov.uk
@SDDC on Twitter
@southderbyshiredc on Facebook

Please ask for Democratic Services
Phone (01283) 595722/ 595889
Democratic.services@southderbyshire.gov.uk

Our Ref
Your Ref

Date: 27 September 2023

Dear Councillor,

Finance and Management Committee

A Meeting of the **Finance and Management Committee** will be held at **Council Chamber**, Civic Offices, Civic Way, Swadlincote, DE11 0AH on **Thursday, 05 October 2023** at **18:00**. You are requested to attend.

Yours faithfully,

Chief Executive

To:- **Labour Group**
Councillor R Pearson (Chair), Councillor L Singh (Vice-Chair)
Councillors S Harrison, M Mulgrew, G Rhind, B Stuart, S Taylor and N Tilley.

Conservative Group
Councillors D Corbin, M Fitzpatrick, M Ford and S Meghani

Liberal Democrats
Councillor G Andrew

AGENDA

Open to Public and Press

1	Apologies and to note any substitutes appointed for the Meeting.	
2	To receive the Open Minutes of the meeting held on:	
	16 March 2023	**4 - 9**
3	To note any declarations of interest arising from any items on the Agenda	
4	To receive any questions by members of the public pursuant to Council Procedure Rule No.10.	
5	To receive any questions by Members of the Council pursuant to Council procedure Rule No. 11.	
6	Reports of Overview and Scrutiny Committee.	
7	BUDGET SETTING APPROACH 2024-25	**10 - 15**
8	DEVOLUTION RETROFIT FUNDING	**16 - 54**
9	MEMBER ICT PROTOCOL	**55 - 100**
10	COMMITTEE WORK PROGRAMME	**101 - 106**

Exclusion of the Public and Press:

11 The Chair may therefore move:-

That in accordance with Section 100 (A)(4) of the Local Government Act 1972 (as amended) the press and public be excluded from the remainder of the Meeting as it is likely, in view of the nature of the business to be transacted or the nature of the proceedings, that there would be disclosed exempt information as defined in the

paragraph of Part I of the Schedule 12A of the Act indicated in the header to each report on the Agenda.

12 To receive the Exempt Minutes of the meeting held on:

16 March 2023

13 To receive any Exempt questions by Members of the Council pursuant to Council procedure Rule No. 11.

14 SHARPE'S POTTERY HERITAGE AND ARTS TRUST

15 WRITE-OFF COUNCIL TAX, BUSINESS RATES, BENEFIT OVERPAYMENT

16 LONG TERM LEASE OF SHARDLOW ALLOTMENTS TO SHARDLOW AND GREAT WILNE PARISH COUNCIL

17 REGRADE OF POST - PROJECT OFFICER ENVIRONMENT (HO132)

OPEN

FINANCE AND MANAGEMENT COMMITTEE

16 March 2023

PRESENT:

Labour Group
Councillor Pearson (Chair), Councillor Rhind (Vice-Chair) and Councillors Tilley, Richards, Southerd and Taylor.

Conservative Group
Councillors Dawson, Ford, Lemmon, Patten (substitute for Councillor Fitzpatrick), Smith and Watson.

Non-Grouped
Councillor Churchill.

In Attendance
Councillor Wheelton

FM/130 **APOLOGIES**

The Committee was informed that apologies had been received from Councillor Fitzpatrick (Conservative Group).

FM/131 **TO RECEIVE THE OPEN MINUTES OF THE FOLLOWING MEETINGS:**

The Open Minutes of the Audit Sub-Committee meetings held on 16 March 2022, 22 June 2022, 7 September 2022 and 7 December 2022 were noted, approved as a true record and signed by the Chair.

FM/132 **DECLARATIONS OF INTEREST**

The Committee was informed that declarations of personal interest had been received from Councillor Taylor and Councillor Smith regarding item FM/142 by virtue of being Parish Councillors.

FM/133 **QUESTIONS FROM MEMBERS OF THE PUBLIC PURSUANT TO COUNCIL PROCEDURE RULE NO 10**

The Committee was informed that no questions from members of the public had been received.

FM/134 **QUESTIONS BY MEMBERS OF THE COUNCIL PURSUANT TO COUNCIL PROCEDURE RULE NO 11**

The Committee was informed that no questions from members of the council had been received.

FM/135 **REPORTS OF OVERVIEW AND SCRUTINY**

The Committee was informed that no reports from the Overview and Scrutiny Committee had been received.

FM/136 **CORPORATE PLAN 2020-24 PERFORMANCE REPORT (2022-2023 QUARTER 3 – (1 APRIL TO 31 DECEMBER)**

The Head of Organisational Development and Performance presented the report to the Committee highlighting the key aims of the plan and eleven corporate measures for this Committee all of which were on track. There were no changes to the status of the risks within the register, but a new risk had been included for the audit of the Council's accounts in quarter three. There were no changes to the Chief Executive's risk register.

RESOLVED:

1.1 The Committee approved progress against performance targets set out in the Corporate Plan 2020 - 2024.

FM/137 **REVENUE FINANCIAL MONITORING 2022-23**

The Head of Finance presented the updated report to the Committee noting that the overall deficit was down for the year end and that the outturn was consistent with quarter two. It was noted that the underspend on Revenues and Benefits would change due to increased audit fees over the next three years.

RESOLVED:

1.1 The Committee considered and approved the latest revenue financial position for 2022/23 as detailed in the report.

1.2 The Committee considered and approved the updated Medium Term Financial Plan.

FM/138 **HOUSING REVENUE ACCOUNT REVENUE FINANCIAL MONITORING 2022-23**

The Head of Finance addressed the Committee and confirmed that there were no updates to the financial plan adding that quarters two and three were consistent and that there were no changes to the outturn position. The £400,000 overspend was due to planned maintenance contracts, an impact on reserves for 2026-27 and a loss in budgeted rent.

Members looked forward to seeing the number of void properties reduce and noted that some properties were being reinspected for asbestos content in the floor tiles. The Strategic Director (Corporate Services) confirmed that there was an up-to-date Risk Register for asbestos.

RESOLVED:

1.1 The Committee considered and approved the latest revenue financial position for 2022/23 as detailed in the report.

FM/139 **COLLECTION FUND 2022-23**

The Head of Finance presented the report to the Committee confirming that the position with the fund was unchanged since last quarter.

RESOLVED:

1.1 The Committee considered and approved the latest Collection Fund position as detailed in the report.

FM/140 **CAPITAL FINANCIAL MONITORING**

The Head of Finance presented the report to the Committee highlighting that there were no updates from the previous quarter, but noted that Section 106 funding should be considered.

Councillor Smith sought assurance that the Gulley Cleaner purchased was fit for purpose. The Head of Operational Services and the Head of Finance would clarify and report back. Councillor Churchill asked if capital allowances would be used to purchase used equipment to which the Head of Finance confirmed this would be appropriate.

RESOLVED:

1.1 The Committee considered and approved the latest capital financial position for 2022/23 as detailed in the report.

1.2 The Committee noted the balance of Section 106 Agreement funding available for use by the Council for capital projects as detailed in Appendix 2 of the report.

FM/141 **TREASURY MANAGEMENT UPDATE 2022-23**

The Head of Finance presented the report to the Committee highlighting no changes although the CCLA fund bid price dropped this was a long-term investment with a good return in interest.

Councillor Churchill asked if any of the Council's investments would be exposed to the current financial crises. The Head of Finance confirmed that all the Council's investments were safe. Councillor Smith requested a notification for the benefit of residents regarding the Council's investments. The Chair confirmed that a statement would be prepared to respond to any enquiries received from the public.

RESOLVED:

1.1 The Committee considered and approved the latest Treasury Management Update for quarter 3 2022/23 as detailed in Appendix 1 of the report.

1.2 The Committee approved the updated Counterparty List for investments and bank deposits as detailed in Appendix 2 to the report.

FM/142 **CONCURRENT FUNCTION – UNSPENT ALLOCATIONS**

The Strategic Director (Corporate Resources) presented the report to the Committee and noted that twelve of 31 Parishes in South Derbyshire had underspent their allocations.

Members discussed options for providing advice and guidance to Parish Councils and Clerks on how to spend their allocations and to encourage the use of Section 106 funding. Members suggested using the annual meeting for Parish Councils, Derbyshire Association of Local Councils and the Area Forums as means of communicating help and assistance. Members agreed to review a report of all unspent funding at a later Committee.

RESOLVED:

1.1 The Committee considered the proposals from Parish Councils to utilise unspent allocations of Concurrent Functions relating to previous years as detailed in the report.

1.2 The Committee noted that any payments approved in 1.1 above, be dependent upon evidence of expenditure incurred.

1.3 The Committee agreed that future allocations paid to Parishes be subject to a review in 2023/24.

FM/143 **COMMITTEE WORK PROGRAMME**

The Strategic Director (Corporate Resources) presented the report to the Committee.

RESOLVED:

The Committee considered and approved the updated work programme.

FM/144 **LOCAL GOVERNMENT ACT 1972 (AS AMENDED BY THE LOCAL GOVERNMENT [ACCESS TO INFORMATION] ACT 1985)**

RESOLVED:

That, in accordance with Section 100(A)(4) of the Local Government Act 1972 (as amended), the press and public be excluded from the remainder of the Meeting as it is likely, in view of the nature of the business to be transacted or the nature of the proceedings, that there would be disclosed exempt information as defined in the paragraphs of Part 1 of the Schedule 12A of the Act indicated in brackets after each item.

QUESTIONS BY MEMBERS OF THE COUNCIL PURSUANT TO COUNCIL PROCEDURE RULE NO 11

The Committee was informed that no questions had been received.

SUNDRY DEBTOR WRITE OFFS

RESOLVED:

The Committee approved the recommendations in the report.

ROSLISTON FORESTRY CENTRE UPDATE

RESOLVED:

The Committee approved the recommendations in the report.

LEISURE MANAGEMENT CONTRACT PROCUREMENT

RESOLVED:

The Committee approved the recommendations in the report.

LONG TERM LEASE TO ROSLISTON, SEALES AND LINTON SCOUT GROUP

RESOLVED:

The Committee approved the recommendations in the report.

COMMUNITIES TEAM SERVICE ASSISTANT

RESOLVED:

The Committee approved the recommendations in the report.

REVIEW OF OPERATIONAL SERVICES STRUCTURE

RESOLVED:

The Committee approved the recommendations in the report.

MECHANIC SALARY AND FLEET MAINTENANCE

RESOLVED:

The Committee approved the recommendations in the report.

SERVICE LEVEL AGREEMENT RELATING TO CONSERVATION ADVICE

RESOLVED:

The Committee approved the recommendations in the report.

The meeting terminated at 18:55 hours

COUNCILLOR R PEARSON

CHAIR

REPORT TO:	**FINANCE AND MANAGEMENT COMMITTEE**	**AGENDA ITEM: 7** **CATEGORY: DELEGATED**
DATE OF MEETING:	**05 OCTOBER 2023**	
REPORT FROM:	**STRATEGIC DIRECTOR (CORPORATE RESOURCES)**	**OPEN**
MEMBERS' CONTACT POINT:	**CHARLOTTE JACKSON** Charlotte.jackson@southderbyshire.gov.uk	**DOC:** s/finance/committee/2023-24/September
SUBJECT:	**BUDGET SETTING APPROACH 2024-25**	
WARD(S) AFFECTED:	**ALL**	**TERMS OF REFERENCE: FM08**

1.0 Recommendations

1.1 That the Committee notes the budget setting approach within the report and Members provide feedback accordingly to the Strategic Director (Corporate Resources).

2.0 Purpose of the Report

2.1 To consult Members on the approach for setting the 2024/25 budget.

3.0 Detail

INTRODUCTION

3.1 This report seeks feedback from Members on the proposed approach for setting the Council's budget for 2024/25, including any budget proposals Members wish to instruct officers to consider and develop.

BACKGROUND

3.2 The Local Government Act 1992 requires the councils that are billing authorities complete and approve their budgets and set a council tax before 11 March immediately prior to the start of the financial year on 1 April.

3.3 Officers have now started to review the detailed income and expenditure budgets by service for the forthcoming 2024/25 financial year across all its operations – the General Fund and Housing Revenue Account (HRA) revenue accounts and the General Fund and HRA Capital Programmes.

3.4 The Strategic Director (Corporate Resources) has set out some early budget setting principles for services to work with (see below).

3.5 The purpose of this report is to consult Members on any further features or principles they would like to set as part of determining next year's budget, to ensure that proposals are considered in the context of the overall budget position and affordability. The early discussion also provides an opportunity for Members to instruct officers to consider and develop budget proposals.

KEY PRINCIPLES TO DEVELOPING BUDGET PROPOSALS

3.6 The three key principles set out to Managers in preparing their budgets for next year are:

3.6.1 Budgets should support Service Plan and the Council Plan - Overall, services should align with Service Plans and the Council Plan. This is a fundamental principle to ensure that appropriate funding is in place. It will also reduce and remove the need for further reports to committee for additional funding requests, unless there are specific requests from members on this or there are other requirements around procurement or other approval considerations.

3.6.2 Revenue investment should be based on demonstratable need or be self-funding - This means that any cost-pressures (such as inflation pressures on supplies, services, and contracts), additional staff or reductions in income due to lower demand or reduced fees, should, insofar as is possible, be "self-funding". This means services should try as far as is reasonably practical to off-set increases in financial resources by making savings in other areas or alternatively, additional revenue investments should be fully demonstrated.

Overall, proposals will need to demonstrate an evidence-based business case which sets out the service need and how additional revenue funding will seek to meet that need, and where possible, reduce ongoing expenditure or increase income in other areas.

3.6.3 Capital growth will be considered based on need and innovation meaning it is essential for the maintenance of service delivery or will improve service delivery by way of revenue improvement - Ideally, if we are creating or enhancing an asset, it should be because it will improve the council's financial position through reducing spend or generating income, or it must be because we need to do this to maintain services.

Again, this requires services to document and demonstrate a sound business case and evidence service investment need.

THE BUDGET SETTING APPROACH

3.7 There are several other features of the budget process that are different this year or that are important for members to have an understanding of and these are set out below.

3.8 The first key feature is that the budget will be set using an "incremental budgeting" approach. This is where the current year's budget is taken forward into the new year, adjusted for changes presented to members and subsequently approved.

3.9 As such, all budgetary changes, will be set out in reports. This will be the case for individual changes above a de-minimis level of £5k, but for amounts lower than £5k, all service area changes will be consolidated and reported as "de-minimis changes", by directorate.

3.10 Proposals around additional staffing resource will be set out clearly so that proposed increases to the establishment are well understood.

3.11 Similarly, proposals around variations to fees and charges will set out the basis of any changes and the resultant impact to income.

3.12 It is envisaged that, since proposals are to be presented in a way that identifies a clear business need, there will be a forthcoming reduction in any need for further reports to committee for additional funding requests. However, it is recognised that there may be specific requests from committees to sign off at future proposal milestones, receive updates on the progress of new initiatives, or other requirements, such as procurement award sign off.

3.13 To ensure effective financial scrutiny, early member engagement on the budget is being undertaken, starting with this context setting report. Engagement with each of the committees is proposed to be held with Environmental and Development Services Committee (ED&S) on 21 September 2023, Housing and Community Services Committee (H&CS) on 28 September 2023, Finance and Management Committee (F&MC) on 5 October 2023 and Overview and Scrutiny (O&SC) on 11 October 2023.

3.14 A draft budget position will then be prepared and presented to F&MC at its 23 November meeting. The Committee will agree the draft budget for approval to commence the public and statutory consultation.

3.15 During January, the draft budget will be presented to policy committees and O&SC. The reports will present the consolidated draft budget and individual proposals to give each policy committee the holistic view of the Council's finances and affordability considerations, as well as the committee specific detail.

3.16 In the past, public consultation has been achieved through Area forums. This year, the process will be expanded to include online consultation, to run for 6 weeks. Feedback from the consultations will be reported to F&MC at its meeting on 15 February, alongside feedback and changes made as a result of policy

committee review. F&MC will review the final proposed budget considering consultation feedback and make its recommendations to Council for final approval.

MEDIUM TERM FINANCIAL PLANNING

3.17 The Council's current Medium Term Financial Plan (MTFP) includes provision for growth and inflationary demands. The assumptions and associated financial risks are considered as a worst-case scenario and there are recurring budget gaps being met by reserves over the life of the plan.

3.18 As the budget is developed, the plan will be reviewed and renewed to align with the new proposed budget from 2024. The review will include the assessment of all assumptions that drive the future financial forecasts in the plan as well as the creation of the worst- and best-case scenarios against a "base case" to set out the most likely outcome.

3.19 A new Medium Term Financial Strategy will also be developed later into the budget setting timetable and presented alongside the budget for approval in February. This overarching strategy will consider the future funding expectations and opportunities for increasing the Council's self-sufficiency in the light of diminishing central government grants and an uncertain future funding outlook and a cycle of recurrent 1-year local government funding settlements, whilst ensuring the Council can continue to fund and deliver excellent services.

TIMETABLE

3.20 The proposed timetable is as follows:

Date & Committee	Milestone
21 September – E&DS 28 September – H&CS 5 October – F&MC 11 October – O&SC	Consultation on budget setting principles/values and budget changes/proposals for development
September – November	*Budgets scoped and reviewed by officers and Leadership Team*
23 November – F&MC	Consideration of consolidated budget and individual proposals Approval to consult
4 January – E&DS 8 January – H&CS 11 January – F&MC 17 January – O&SC	Committee review of consolidated budgets and individual proposals relevant to Committee service budget **Draft MTFS presented to O&SC**
24 November – end January	Statutory and public consultation with ratepayers (businesses) and residents

15 February – F&MC	Review of final consolidated budget, review of consultation responses **Draft MTFS**
28 February – Council	Final approval of Budget and Council Plan **Final MTFS**

SUMMARY

3.21 Feedback is sought on the overall approach and main features of the budget setting timetable, the key principles, the proposed public consultation and any other areas of the budget Member wish to see developed.

4.0 Financial Implications

4.1 None currently.

5.0 Corporate Implications

Employment Implications

5.1 None.

Legal Implications

5.2 None.

Corporate Plan Implications

5.3 None

Risk Impact

5.4 None

6.0 Community Impact

6.1 None currently.

Equality and Diversity Impact

6.2 None.

Social Value Impact

6.3 None.

Environmental Sustainability

6.4 None.

7.0 Background Papers

7.1 None

REPORT TO:	**FINANCE AND MANAGEMENT COMMITTEE**	**AGENDA ITEM: 8**
DATE OF MEETING:	**05 OCTOBER 2023**	**CATEGORY: RECOMMENDED**
REPORT FROM:	**STRATEGIC DIRECTOR (SERVICE DELIVERY)**	**OPEN**
MEMBERS' CONTACT POINT:	**CRAIG LODEY, 07435 766937, craig.lodey@southderbyshire.gov.uk**	**DOC:**
SUBJECT:	**DEVOLUTION RETROFIT FUNDING**	
WARD(S) AFFECTED:	**ALL**	**TERMS OF REFERENCE: FM08**

1.0 Recommendations

1.1 To accept a Grant offer of £583,500 from Midlands Net Zero Hub to fund low carbon retrofit measures to be installed at social and private housing across South Derbyshire on the terms of the Grant Agreement **(Appendix A).**

1.2 To authorise the Chief Executive in consultation with the Chair of the Finance and Management Committee to negotiate changes to and revisions of the programme, milestones and Grant Agreement.

2.0 Purpose of the Report

2.1 This report is intended to seek approval from members to accept the Grant Offer of £583,500 to fund energy improvement measures on residential properties in South Derbyshire.

3.0 Executive Summary

3.1 This report seeks to outline the recent offer of £583,500 of funding to South Derbyshire District Council made by the Midland Net Zero Hub (Nottingham City Council) to install energy efficiency measures in homes within the district.

3.2 The funding may be regarded as complementary to funds already received or committed by Midland Net Zero to existing LAD3 and HUG2 funding but has no co-dependencies with those funds.

3.3 Funds can be used to support the installation of energy efficiency measures on both private and social housing.

4.0 Detail

4.1 In preparation for the Combined Authority the Department for Levelling Up, Housing and Communities (DLUHC), has allocated a total of £18m of capital funding to Derbyshire County Council as the Lead Funder on behalf of the four Constituent Councils of the EMCAA, if the grant is approved Midland Net Zero Hub (Nottingham City Council) will received a total of £16M. The total award is to be distributed equally

between the 15 District and Borough Councils in the region and the 2 City Councils and are intended to bridge the funding gap that currently exists where households who need support but are not receiving support due to the stringent criteria of the national funding schemes such as HUG2 that is exclusive to 'off-gas' property. The intervention will also better allow a place-based approach enabling Local Authorities in the region to identify key areas of need, or to fill in the gaps of existing programmes LAD3 or SHDF Wave 2.1.

4.2 For each of the constituent councils the overall objectives set by the scheme are;-

- To undertake 'whole house' retrofit on 5 properties
- Install measures to comply with PAS2035:2019 to 36 properties
- To improve the health and wellbeing of home occupiers through pre and post survey assessment
- Reduced energy consumption and lower carbon footprint
- Reduce the number of households at EPC band D or lower
- Effect a net improvement in SAP rating

4.3 Funds could also be utilised for additional measures in properties that further increases EPC rating and prevents repeat visits under future schemes minimising disruption and maximising benefits for the occupiers.

4.4 The funding can be used to carry out works on private, private rented and social housing.

4.5 Measures might include insulation, energy efficient windows and doors and improved ventilation. Where indicated by retrofit design low carbon heating measures such as Air Source Heat Pumps, Solar photovoltaics or battery storage may be appropriate.

4.6 The works must be carried out by contractors with PAS2030 accreditation and in accordance with the process set out in PAS2035.

4.7 Works can be carried out to complement measures being installed under other energy efficiency schemes such as SHDF or HUG but funding cannot be used to subsidise a single measure already funded by another scheme.

4.8 Delivery plan

Subject to refinement the delivery plan has been developed on known information or anticipated demand. Based on existing commitments and experience gained in earlier initiatives, the programme, delivery has been structured to allow time to more carefully select property suitable for 'whole house' retrofit and avoid unforeseen costs that those homes may present.

	Eligible homes signed up to receive measures	**Whole Retrofits completed**	**Other measures installed***	**Number of homes that improve to a EPC band C or above**	**Number of homes that have been improved by at least 1 EPC band from a starting SAP 1-54 rating (EPC-EFG)-170**
	Forecast	**Forecast**	**Forecast**	**Forecast**	**Forecast**
2023/24					
Q1					
Q2	0	0	0	0	0
Q3	20	0	0	0	0
Q4	20	0	15	10	15
2024/25					
Q1	36	**0**	36	28	30

Q2	36	**3**	36	36	36
Q3	36	**5**	36	36	36
Q4					

4.9 The delivery plan is provisional and some degree of flex is anticipated by the funder.

4.10 This offer presents an opportunity for the housing department to undertake energy efficiency works that would otherwise be funded by the planned maintenance budget or from reserves.

4.11 Undertaking 'Whole house' retrofit on a home that is tenanted would be highly disruptive to the residents. The Council does not have a pool of property into which sitting tenants can be decanted or a budget to make appropriate compensatory payments for disturbance therefore it is proposed that this type of work is only carried out on suitable properties that are currently void.

4.12 The offer allows the opportunity to carry out energy efficiency works on private residential property that cannot be treated under the LAD3 or HUG2 schemes.

5.0 Financial Implications

5.1 This grant is not subject to any co-funding conditions.

5.2 An upfront payment of 20% of the funding will be provided with the balance paid on delivery progress being acheived.

5.3 The grant spend profile is to be agreed between Nottingham City Council (the funding body) and South Derbyshire District Council. The following table indicates how the grant would be spent based on known work and commitments.

FY	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
2023-24								10k	15k	15k	10k	50k	£583,5
2024-25	£100k	£50k	£133.5k	£100k	£100k								

5.4 The Council will retain all financial records relating the expenditure

5.5 The funding is regarded as Capital expenditure and not revenue.

5.6 The MOU contains a list of expenditure that is not eligible and the scheme is subject to an assessment of eligible expenditure and a monthly reconciliation report is required.

5.7 The Contractor appointed to deliver the works funded by the Grant Funding must be properly procured. As they are competant to complete to the PAS2030 and PAS2035 standard it is anticipated that retrofit works will be undertaken by the contractors already delivering the SHDF and HUG works however SDDC will consult with DSFS Procurement Team to ensure compliance with procurement rules.

6.0 Corporate Implications

Employment Implications

6.1 This funding is additional to existing programs and places an obligation on council officers to select suitable property and deliver in line with the scheme objectives. However, using the skills of existing officers but this is felt to be achievable and therefore no additional resource is necessary.

Legal Implications

6.2 The funder will cease payment or demand repayment if; -

- The agreed programme milestones are not met or the Funder perceives that progress is slow
- The grant funding is not used for the purposes for which the scheme has been set designed.
- The Council has in the opinion of the Funder breached subsidy control rules.

6.3 The funder requires an Information Sharing Agreement to be agreed. This is only to be invoked in the event that the Funder changes the reporting requirement.

6.4 The Council must report any incidence where financial mismanagement or fraud is suspected.

6.5 The Grant Conditions are stringent and can result in claw back. This will expose the Council to financial and reputational risk.

6.6 Officers will need to take advice as to whether each payment made under the MOU is complaint with Subsidy Control Rules

Corporate Plan Implications

6.7 This funding would assist the Council's commitment to achieving its corporate net zero target.

6.8 The funding of energy efficiency measures will improve the living conditions of residents in council accommodation.

Risk Impact

6.9 The Council is already engaged on delivering significant SHDF and HUG projects and has experienced delays resulting from insufficient capacity in the retrofit industry to complete works to PAS2030/2035 standards.

6.10 The Grant funding would add additional workload on officers delivering the existing programmes especially when considering the whole house retrofit works.

6.11 During the delivery of 'Whole House retrofit' it can be anticipated that works additional to those previously identified will be found to be required and that this may entail additional cost that could prejudice the overall budget.

6.12 The Council's recent experience with PAS2030/ 2035 equips it well to understand the issues and risks attendant on retrofit works and to mitigate these to an acceptable level.

7.0 Community Impact

Consultation

7.1 As there is an existing reserve of LAD3 applications there is no requirement to advertise this award or consult widely.

7.2 Council housing residents are already engaged with SHDF programme and the communication strategy is in place. Work on void property requires no specific consultation with residents.

Equality and Diversity Impact

7.3 There are no implications for equality and diversity.

Social Value Impact

7.4 This award will allow the council to install energy efficiency measures at homes that could not be completed under the LAD3 scheme due to budget and delivery constraints.
7.5 The award will allow the council to undertake 'whole house' retrofit works on a small number of its void properties that would otherwise not be carried out for budgetary reasons.
7.6 The award may be used to support 'whole house' retrofit on privately owned property that Environmental Services may have considered un-viable using existing funding sources.
7.7 Improved health, comfort and financial wellbeing of our stakeholders.

Environmental Sustainability

7.8 The initiative is concerned with delivering energy efficiency and low carbon heating solutions that are intended to reduce carbon emissions and therefore is aligned with the Council's stated policy to achieve net zero by 2030.
7.9 There are no adverse impacts on environmental sustainability.

8.0 Conclusions

8.1 This funding is offered with few conditions.
8.2 The funding requires no Council co-funding commitment.
8.3 The programme can be delivered by existing Council officers and no additional resource.
8.4 The funds can be utilised to improve the council's own social housing stock and so reducing pressure on the planned maintenance budget.
8.5 The funding can be used to fill the gap created between applications for LAD3 improvements, the funding available and the lack of a follow-on LAD4 scheme.

9.0 Background Papers

Appendix A – Memorandum of Understanding

Grant Confirmation Document

Project Name: East Midlands Domestic Retrofit

Project Sponsor:

Between:

1. Nottingham City Council

2. South Derbyshire District Council

Dated this ******

THIS CONFIRMATION OF GRANT is made on the date appearing on the front page of this document and is made between:

(1) **NOTTINGHAM CITY COUNCIL** as Funder (managing the funding distribution), whose principle place of business is at Loxley House, Station Street, Nottingham, NG2 3NG ("**the Funder**"); and

(2) **SOUTH DERBYSHIRE DISTRICT COUNCIL**– Civic Offices, Civic Way, Swadlincote, DE11 0AH, (**the "Recipient**")

BACKGROUND:

A The Funder, in exercising its statutory powers, has received confirmation of in principle grant funding from th-e Lead Funder in respect of the Project.

B The Funder has agreed to make the Grant available to the Recipient for the purposes of financially assisting the Project subject to the terms of this agreement.

C This agreement sets out the terms and conditions on which the Grant is made by the Funder to the Recipient in respect of the Project.

D These terms and conditions are intended to ensure that the Grant is used for the purpose for which it is awarded.

1. DEFINITIONS

1.1. In this Confirmation Document the following words shall have the following meanings:

"Applicable Legislation"	any Law relating to the Project including the Environmental Information Regulations 2004 the Freedom of Information Act 2000 and the Equality Act 2010.
"Application"	The Recipient's application for Grant.
"Approval" and "Approved"	the written approval of the Funder.
"Confirmation Document"	this document including the schedules and appendices attached to it.
"Condition Period"	the period of ten years from the date of this Confirmation Document.
"Condition"	a condition of this Confirmation Document.
"Confidential Information"	any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information which relates to the business, affairs, properties, assets, trading practices, services, developments, trade secrets, Intellectual Property Rights, know-how, personnel, customers and suppliers of either Party, all personal data and sensitive personal data within the meaning of the Data Protection Act 2018 and commercially sensitive information in accordance with the Freedom of Information Act 2000.
Constituent Councils	Derbyshire County Council, Derby City Council, Nottinghamshire County Council, Nottingham City Council
" Data Protection Legislation"	(i)The General Data Protection Regulation as enacted into English law by the Data Protection Act 2018, as revised and superseded from time to time (GDPR); (ii) Directive 2002/58/UK as updated by Directive 2009/136/UK; and (iii) any other laws and regulations relating to the processing of personal data and privacy which apply to a party and, if applicable, the guidance and codes of practice issued by the relevant data protection or supervisory authority.
"Delivery Partner"	any third party or parties appointed or funded by the Recipient to deliver the Project using the Grant.
EMCCA	East Midlands County Combined Authority
"Environmental Information Regulations" or "EIR"	the Environmental Information Regulations 2004 (SI 2004/3391) together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such regulations.
"Encumbrance"	any mortgage, charge, pledge, lien or other encumbrance.
"Event of Default"	as described in clause 6.
"FOIA"	as described in Clause 12.2.

"Grant"	the grant in the maximum amount payable to the Recipient under this Confirmation Document, in the proportions and on the dates as set out in the Schedules.
"Grant Conditions"	the MoU and any related documents issued to the Funder by the Lead Funder, including from time to time, agreed changes to the Grant Conditions and any subsequent grant determination letters and other related documents issued by the Lead Funder to the Funder.
"Insolvent"	if the Recipient is unable to pay debts as they fall due, or is deemed under Applicable Law to be so, or that it has an excess of liabilities over assets (taking into account contingent and prospective liabilities) and/or the "winding up" of a person include, where such person is or comprises a person other than a company (as defined in the Companies Act 1985), any corresponding process applicable to that person.
"Intellectual Property Rights"	Means any patent, copyright, design right, registered design, database right, trade mark, service mark, know-how, utility model, unregistered design or, where relevant, any application for such right, know-how, trade or business name, domain name or other similar right or obligation whether registerable or not or other industrial or intellectual property right subsisting in any territory or jurisdiction in the world and "Intellectual Property" shall be construed accordingly.
"Lead Funder"	Derbyshire County Council on behalf of the four Constituent Council, who will form the East Midlands Mayoral Combined County Authority, if approved.
"MOU"	the Mobilisation Grant Offer Letter dated XXXXXXX 2023 and issued by the Lead Funder to the Funder in connection with the mobilisation payment for the Scheme.
"Output"	as described in the Schedules to this Confirmation Document.
"Party"	a party to this Confirmation Document and "Parties" shall be construed accordingly.
"Project"	the project described in Schedule 1 and anything necessary to carry out the Project.

2. INTERPRETATION

2.1. References to Parties and other persons include their successors and permitted assigns, except where the context requires otherwise.

2.2. References to a "Clause" or "Schedule" are references to a clause of, or a schedule to this Confirmation Document unless otherwise provided. Clause headings are for ease of reference only.

2.3. References to this or any other document or statute are references to them in force for the time being and as amended, varied, supplemented, consolidated or re-enacted from time to time and include any schedules or annexes to such document and, in the case of statutes, any delegated legislation. Where there are two or more persons comprised in the "Recipient" then those persons are jointly and severally responsible and liable for all obligations expressed to be assumed by the Recipient

in this Confirmation Document, including for any repayment of Grant or other payment obligation.

2.4. "including" shall be construed so as not to limit the generality of any words or expressions in connection with which it is used.

3. OVERVIEW OF THE SCHEME

In preparation for the Combined Authority the Department for Levelling Up, Housing and Communities (DLUHC), has allocated a total of £18m of capital funding to Derbyshire County Council as the Lead Funder on behalf of the four Constituent Councils who will form part of the EMCAA, if approved.

4. THE RECIPIENT'S OBLIGATIONS

4.1. The Recipient will carry out the Project in the manner set out in Schedule 1.

4.2. The Recipient will be reimbursed as agreed and set out in Schedule 2.

4.3. The Recipient will deliver the Targets and Outputs as set out in Schedule 3.

4.4. The Recipient will co-operate with the Monitoring and Evaluation requirements more particularly described in Schedule 5.

4.5. The Recipient shall:

4.5.1. not, other than as agreed by the parties and described in Schedule 1, during the Condition Period without the Funder's consent, create or permit to subsist any Encumbrance on any of its interest in any of its assets or revenues relating to the Project except for liens arising by operation of Law;

4.5.2. not, other than as agreed by the parties and described in Schedule 1, during the Condition Period without the Funder's consent (not to be unreasonably withheld) enter into any sale, transfer, lease or other disposal of any or all of its interest in any of the Project assets;

4.5.3. ensure that it has adequate insurance against any actions, claims or demands which may be made against it in respect of the death or injury of any person, or loss of any kind arising to any person who implements, participates in or directly benefits from the Project;

4.5.4. comply with all relevant Applicable Legislation; and

4.5.5. not, at any time during or after the term of the Condition Period, divulge any Confidential Information relating to the performance of this Confirmation Document or the business affairs of the Funder of which the Recipient is, or may become, aware of.

4.6. The Recipient acknowledges that the Funder is subject to the Grant Conditions. The Recipient agrees that it shall, and that it shall ensure that the Delivery Partners shall:

4.6.1. provide such assistance as the Funder reasonably requires to enable it to comply with the Grant Conditions;

4.6.2. not take any action, or fail to take any action that would put the Funder in breach of the requirements of the Grant Conditions (regardless of the enforceability of the Grant Conditions as between the Funder and the Lead Funder);

4.6.3. not take any action or make any omission that causes or may be likely to cause (whether on its own or as part of a series of acts or omissions

committed by the Recipient and/or other parties) or contribute to the Funder to fail to meet the key performance indicators which it is subject to under the MoU;

4.6.4. not take any action or make any omission that causes or would be likely to have a negative impact on the Lead Funder's delivery confidence assessment undertaken in accordance with the MoU;

4.6.5. comply with any processes, procedures and/or ways of working established by the Funder in relation to the Grant or the Project including in relation to information sharing and any other relevant matters in connection with the Grant or Project;

4.6.6. undertake its delivery of the Project, and ensure that any Delivery Partners undertake their duties in a manner consistent with the Code of Conduct and report any breaches or suspected breaches of the Code of Conduct to the Funder immediately on becoming aware of such breach or suspected breach;

4.6.7. comply with all rules, requirements and limitations relating to the use of the Grant set out within the MoU as if they applied directly to the Recipient.

4.6.8. The Recipient accepts and agrees that it shall be responsible for the acts and/or omissions of its Delivery Partners, its subcontractors and the subcontractors of its Delivery Partners as if they were the acts and/or omissions of the Recipient.

4.6.9. The Recipient shall include terms in its agreements with Delivery Partners and subcontractors which give the Recipient sufficient rights to enable the Recipient to comply with its obligations under this agreement.

5. THE FUNDER'S OBLIGATIONS

Subject to this Confirmation Document, and provided always that the Funder has received sufficient funds from the Lead Funder within the life of the Project, the Funder will pay the Recipient in the manner and the amounts set out in Schedule 2.

6. EVENTS OF DEFAULT

6.1. Without prejudice to the other provisions of this Confirmation Document, the following events shall be Events of Default:

6.1.1. **Insolvency** – the Recipient becomes Insolvent;

6.1.2. **Misuse of Grant** – The Recipient applies the Grant otherwise than for the purpose of the Project;

6.1.3. **Poor progress** - successful completion of the Project in accordance with the Project time plan becomes, in either the Funder's reasonable opinion, unlikely to occur;

6.1.4. **Breach of obligation** – at any time, the Recipient fails to perform and observe any obligation owed to the Funder under this Confirmation Document, or under any deed or document supplemental to this Confirmation Document, or creating security pursuant to it;

6.1.5. **Change of the Project's purpose in accordance with this Confirmation Document** – if at any time, the proposed or actual use or operation of the Project ceases to materially comply with the Project particulars as stated in Schedule 1;

6.1.6. **Fraud** – if at any time, the Recipient has acted fraudulently in relation to this Confirmation Document or the Project or any of the beneficiaries or sub-contractors of the Recipient have acted fraudulently in respect of the Project; or

6.1.7. **Material misrepresentation** – if at any time any representation or statement made by or on behalf of the Recipient in this Confirmation Document, the Recipients Application, or in any document referred to in or delivered under this Confirmation Document is not true and accurate in any material respect when made or deemed repeated, whether deliberately or not.

7. WITHHOLDING PAYMENT AND REPAYMENT

7.1. The Lead funder and / or Funder may withhold any or all of the payments of funding, and/or require part of, or the entire amount of funding to be repaid, if:

7.1.1. an Event of Default has occurred;

7.1.2. in the Funder's reasonable opinion, insufficient measures are being taken to investigate and resolve any reported irregularity;

7.1.3. the funding exceeds European Union Subsidy Control limits to the extent that any funding paid should not have been paid, or if a decision of the European Commission or of the European Court of Justice requires payment to be withheld or recovered; or

7.1.4. there is an unsatisfactory report from Funder's auditors indicating fundamental uncertainty, a disagreement or a limitation in Funder's auditors reasonable opinion, an inability to form an opinion, or a report that the statement of funding usage does not give a true and fair view; or

7.1.5. The Recipient, being an unincorporated body, is dissolved or being an incorporated body passes a resolution that it should be wound up, is ordered by the High Court to be wound up, has an administrator appointed by order of the Court, has a receiver or administrative receiver appointed over the whole or any part of its assets, or being a company is struck from the register at Companies House;

7.1.6. in the Funder 's reasonable opinion, the Recipient fails to comply with any requirement of this Confirmation Document;

7.1.7. any necessary consents, (including without limitation planning permission) have not been obtained in relation to the Project;

7.1.8. a charge is taken on an asset financed wholly or partly from Grant monies, without the agreement in advance of Funder;

7.1.9. there is a change in ownership or control of the Recipient other than as set out in this Confirmation Document under the heading 'Background';

7.1.10. in the Funder's reasonable opinion, there is significant change in the nature or scale of the Project; or

8. TERMINATION AND BREACH

8.1. If either Funder or the Recipient materially breaches the provisions of this Confirmation Document (which shall include an Event of Default) then:

8.1.1. if the breach is capable of remedy the party not in breach may serve notice on the other, specifying a period of not more than 28 working days in which

the breach is to be remedied and may not then terminate this Confirmation Document during that period in respect of that breach. If the breach is not remedied within that period, the matter will be referred to mediation in accordance with the dispute resolution procedure set out below;

8.1.2. if the breach is not capable of remedy, then the party not in breach may terminate this Confirmation Document by giving immediate written notice;

8.1.3. if the Recipient breaches the provisions of this Confirmation Document, the Funder may withhold any sum due, or at any time thereafter due, to the Recipient pending remedy of the breach, but this shall not prejudice the Funder's other rights under this Confirmation Document, or otherwise existing at law; or

8.2 if the output's set out in this Confirmation Document have not been met, or, are unlikely to be me , or, are unlikely to be met (and such breach shall be considered as an Event of Default).

9. RECOVERY OF SUMS DUE

9.1. The Funder may, by notice in writing to the Recipient, set-off against any liability of the Recipient to repay monies to it under this Confirmation Document (whether liquidated or un-liquidated and whether actual or contingent) the amount of any payment owed or payable by the Funder to the Recipient.

9.2. Any overpayment by the Funder to the Recipient shall be a sum of money recoverable by the Funder from the Recipient.

9.3. The Recipient shall make any payments due to the Funder without any deduction.

9.4. The payment of the Grant by the Funder under this Confirmation Document is believed to be outside the scope of Value Added Tax, but if any Value Added Tax shall become chargeable, then all payments of funding shall be deemed to be inclusive of all Value Added Tax, and the Funder shall not be obliged to pay any Value Added Tax over and above the agreed funding.

10. ASSIGNMENT AND SUB-CONTRACTING

10.1. The Recipient may not assign the whole or any part of their rights nor delegate the whole or any part of their obligations under this Confirmation Document without the prior written consent of the Funder.

10.2. This Confirmation Document shall benefit and be binding on the Parties, their respective successors and assigns or other body which may become the successor of DLUHC or such similar Government Department.

11. QUALITY

Where operation in accordance with a quality standard has been confirmed by the Recipient Application, the Recipient shall at all times comply with that quality standard and shall maintain accreditation with any relevant quality standard authorisation body relevant to the Project. To the extent that a standard of work has not been specified in relation to the Project, the Recipient shall use the best applicable techniques and

standards and carry out the Project with all reasonable care, skill and diligence and in accordance with good practice.

12. CONFIDENTIALITY

12.1. All documents and information received by the Recipient during or in connection with the performance of the Project from the Funder, or any person employed by them, shall be held in confidence.

12.2. Such documents and information shall not be disclosed by the Recipient or their staff or agents, to any other person without the permission of the Funder unless a duty to disclose to that person is imposed under statute or by court order or under the Freedom of Information Act 2000 ("**FOIA**").

12.3. The Recipient shall each take all reasonable steps to ensure that its staff are aware of and comply with this obligation of confidence.

12.4. The Funder may disclose such information concerning the Project and the Recipient to third parties as it thinks fit, except for Confidential Information.

13. WAIVER

The failure of any Party to insist upon strict performance of any provision of this Confirmation Document or the failure of any Party to exercise any right or remedy shall not constitute a waiver of that right or remedy and shall not cause a diminution of the obligations established by this Confirmation Document. No waiver shall be effective unless it is expressly stated to be a waiver and communicated to the other Parties in writing.

14. VARIATION

14.1 In the event that the Parties agree that changes to the Project are required (for example, to add or remove an activity or Output, to increase or decrease the quantity of an activity or Output, or to change the order in which the activities are to be performed or the locations where the activities are to be provided) then such changes (including any change in the amount or timing of funding) will be negotiated between the Parties. Any changes to the Project will be recorded in writing by the Parties and appended to this Confirmation Document.

15. SEVERABILITY

15.1. If any provision of this Confirmation Document is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed and the remainder of the provisions of the Confirmation Document shall continue in full force and effect as if the Confirmation Document had been executed with the invalid, illegal or unenforceable provision eliminated.

15.2. In the event of a holding of invalidity so fundamental as to prevent the accomplishment of the purpose of the Confirmation Document the Funder and the Recipient will immediately commence negotiations in good faith to remedy the invalidity.

16. FORCE MAJEURE

Neither Party shall be liable for failure to perform its obligations under this Confirmation Document if such failure results from national war, emergency

regulation or any other circumstances beyond that Party's reasonable control and during such event, no further payments shall be made to the Recipient.

17. INTELLECTUAL PROPERTY RIGHTS

17.1. The Parties agree that all rights, title and interest in or to any information, data, reports, documents, procedures, forecasts, technology, know-how, and any other Intellectual Property Rights whatsoever owned by the Parties before the Commencement Date or developed by any Party during the Condition Period, shall remain the property of that Party.

17.2. Where the Funder has provided the Recipient with any of its Intellectual Property Rights for use in connection with the Project (including without limitation its name and logo), the Recipient shall, on termination of this Confirmation Document, cease to use such Intellectual Property Rights immediately and shall either return or destroy such Intellectual Property Rights as requested by the Funder within 14 days of such a request.

18. PUBLICITY

18.1. The Recipient and the Funder may promote their association with the Project as they think fit.

18.2. The Recipient can install and maintain at each location where the project is based or operates, such signs, commemorative material and other promotional material indicating the involvement of the EMCAA with the project.

19. SUBSIDY CONTROL

19.1. All grant funding is subject to Subsidy Control rules which are part of the Trade and Cooperation Agreement and the Recipient will need to confirm that their project is compliant with these Subsidy Control rules as the Funder accepts no liability with regard to this.

19.2. The Recipient shall comply with and shall ensure that all Delivery Partners shall comply with, all Subsidy Control Rules, and shall ensure that all requirements of the Subsidy Control Rules are met in relation to the Project.

19.3. The Recipient shall not take any action or fail to take any action, or (insofar as it is reasonably within its power) permit anything to occur that will cause the Funder to be in breach of its obligations under the Subsidy Control Rules.

19.4. The Recipient shall provide such reasonable assistance as is requested by the Funder to enable the Funder to comply with its obligations under the Subsidy Control Rules and shall provide information to demonstrate the compliance of the Project when requested by the Funder. No payments shall be made to the Recipient if a decision of a court or any body with responsibility for enforcing the Subsidy Control Rules imposes a requirement for the Funder to withhold and/or recover any funding from the Recipient, or for the Recipient to repay any funding to the Funder.

19.5. The Funder may vary or withhold any or all of the payments and/or require repayment of any Grants already paid or a proportion thereof, together with interest from the date of payment, if:

19.5.1. the representations and warranties made by the Recipient under this agreement do not remain materially true and correct;

19.5.2. variation, repayment, or recovery is, in the reasonable opinion of the Funder, required under or by virtue of the Subsidy Control Rules; or

19.5.3. the Funder or the Recipient is otherwise required to vary, repay, or recover such funding in whole or in part by a court or any body with responsibility for enforcing the Subsidy Control Rules,

and the interest rate payable by the Recipient will be set by the Funder at a level sufficient for the Funder to comply with any such recovery, requirement or obligation.

19.6. The Recipient shall ensure that its Delivery Partners are subject to terms equivalent to those set out in Clauses 19.2 to 19.5.

20. PUBLIC PROCUREMENT

20.1. The Funder as a public body is subject to the Public Contracts Regulations 2015 in respect of the way in which it purchases goods, services and works. As a non-departmental public body it is also keen to promote good practice in purchasing, and follows its own fair purchasing procedures where the amounts expended are below the thresholds for the Public Contracts Regulations 2015 to apply. The Funder is also keen for the organisations it funds to act fairly when spending grant funding.

20.2. Accordingly, when spending money on the Project, the Recipient shall comply (as required) with the Public Contracts Regulations 2015 (or such equivalent legislation as applicable from time to time) and in addition, follow their own financial regulations as well as advertising requirements on the East Midlands Procurement Portal www.eastmidstenders.org and Contracts Finder www.gov.uk/contracts-finder

20.3. For organisations which do not have their own Procurement policies, at the beginning of their respective processes, it is recommended that the Recipient adopts the following procedures according to the estimated value (inc. VAT) of the contract:

Estimated Value for Goods and Services	**Tender Action Required**	**Advertising Requirements**
Below £50,000	Seek three quotations	None
£50,000-£177,897 ,	Formal tender	Advertise tender and award notice through East Midlands Procurement Portal or equivalent
Above £177,897	Formal tender	Advertise tender and award notice on Contracts Finder and Find a Tender (FTS) (Works Contracts advertise on FTD for requirements above £4,447,447 ex VAT))

20.4. The Recipient must then make a decision to purchase on the basis of best value (the optimum combination of whole life costs and the quality to meet that Party's

requirements). The Recipient will also keep records of its decisions and make these available to the Funder upon request.

21. NON-DISCRIMINATION

21.1. The Recipient shall not unlawfully discriminate within the meaning and scope of any law, enactment order or regulation relating to discrimination (whether in race, gender, religion, disability, sexual orientation, age or otherwise) in employment purchasing or the provision of services.

21.2. The Recipient will provide its Equal Opportunities Policy to the Funder on request.

22. FREEDOM OF INFORMATION ACT (FOIA) AND DATA PROTECTION

22.1. The Recipient acknowledges that the Funder are subject to the requirements of FOIA and EIR, and the Recipient (and any sub-contractors or agents) shall assist and cooperate with the Funder to enable the Funder to comply with any information disclosure requirements including providing a copy of all information in its possession or power in the form that the Funder requires within five working days (or such other longer period as may be specified) of the Funder requesting that information.

22.2. The Recipient will use their best endeavours to ensure that requests under the FOIA made direct to the Recipient are transferred to the Funder as soon as practicable after receipt.

22.3. The Funder shall at its sole discretion and without liability determine whether information considered to be by the Recipient as commercially sensitive information and/or any other information:

22.3.1. is exempt from disclosure in accordance with the provisions of the FOIA or the EIR;

22.3.2. is to be disclosed in response to a request for information, and the Recipient shall not respond directly to a request for information unless expressly authorised to do so by the Funder.

22.4. The Recipient acknowledges that the Funder may, under section 45 of FOIA, (and in accordance with the document titled ‘Freedom of Information Code of Practice’ and published under Gov.uk and updated as at July 2018), be obliged under FOIA or the EIR to disclose information without consulting with the Recipient, or following consultation with the Recipient, and having taken their views into account.

22.5. The Recipient shall ensure that all information produced in the course of the Project, or relating to the Project, is retained for disclosure and shall permit the Funder to inspect such records as requested from time to time.

22.6. The Recipient acknowledges that any lists or schedules provided by it outlining Confidential Information, are of indicative value only, and that the Funder may nevertheless be obliged to disclose Confidential Information.

22.7. Where the Recipient is also subject to FOIA and EIR, the Funder shall provide reasonable assistance to it to ensure the Recipient’s compliance with its obligations under such legislation.

22.8. Both parties shall comply with all applicable requirements of and all their obligations under the Data Protection Legislation which arise in connection with the Agreement.

22.9. The Recipient must comply with all applicable requirements of the Data Protection Legislation which arise in connection with this Agreement.

22.10. The Recipient agrees to assist the Funder in securing a compliant data transfer and processing arrangement, including signing such Information Sharing Agreement as

may be set out by the Funder and in addition, where appropriate, anonymising any personal data that it provides to the Funder prior to transfer. No Grant shall be paid until the Funder has received the Recipient's signed Information Sharing Agreement and the Funder is satisfied in its absolute discretion with such other data protection measures as have been taken by the Recipient (without the Funder accepting liability for the adequacy of such measures).

22.11. The Recipient shall comply at all times with the terms of the Information Sharing Agreement.

22.12. The Recipient will indemnify the Funder in full and on demand in respect of any losses that the Funder may suffer as a result of any breaches of Clauses 22.9 – 22.11 by the Recipient.

23. HEALTH AND SAFETY

23.1. If legally required to do so, the Recipient will ensure that they comply with all Health and Safety legislation and will provide their up to date Health and Safety Policy Statements to the Funder on request.

23.2. In circumstances where the Recipient or its respective staff are present on the Funder premises, the Recipient will promptly notify the Funder of any health and safety hazards which may arise during that time, including any incident causing any personal injury or damage to property which could give rise to personal injury.

24. DISPUTE RESOLUTION

24.1. If any dispute arises between the parties out of or in connection with this Confirmation Document or the performance, validity or enforceability of it ("**Dispute**") then the parties shall follow the procedure set out in this clause:

24.1.1. either party shall give to the other written notice of the Dispute, setting out its nature and full particulars ("**Dispute Notice**"), together with relevant supporting documents. On service of the Dispute Notice, each party's authorised representative shall attempt in good faith to resolve the Dispute; and

24.1.2. if the authorised representatives are for any reason unable to resolve the Dispute within 30 days of service of the Dispute Notice, the Dispute shall be referred to the respective parties' Director of Finance and ICT (for the Funder) or Chief Executive Officer (or equivalent) (for the Recipient) who shall attempt in good faith to resolve it.

24.2. If the Dispute is unable to be resolved in accordance with clause 24.1 above, then the parties agree to enter into mediation in good faith to settle the Dispute in accordance with the CEDR Model Mediation Procedure. Unless otherwise agreed between the parties within 20 Business Days of service of the Dispute Notice, the mediator shall be nominated by CEDR. To initiate the mediation, a party must serve notice in writing ("**ADR notice**") to the other party to the Dispute, referring the dispute to mediation. Unless otherwise agreed between the parties, the mediation will start not later than 20 Business Days after the date of the ADR notice.

24.3. No party may commence any court proceedings under clause 31.2 in relation to the whole or part of the Dispute until 20 Business Days after service of the ADR notice, provided that the right to issue proceedings is not prejudiced by a delay.

24.4. If the Dispute is not resolved within 20 Business Days after service of the ADR notice, or either party fails to participate or ceases to participate in the mediation before the

expiry of that 20 Business Days day period, the Dispute shall be finally resolved in accordance with clause 31.2.

25. ENTIRE AGREEMENT

This Confirmation Document constitutes the entire agreement between the Parties relating to the subject matter of the Confirmation Document. This Confirmation Document supersedes all prior negotiations, representations and undertakings, whether written or oral, except that this Clause shall not exclude liability in respect of any fraudulent misrepresentation.

26. RIGHTS OF THIRD PARTIES

Save as expressly set out in this Confirmation Document, a party that is not a Party to this Confirmation Document shall have no rights under it.

27. EXCLUSION

Nothing in this Confirmation Document nor in any other document shall impose any obligation or liability upon the Funder with respect to any actions or obligations or liability assumed or incurred by the Recipient whether under this Confirmation Document, statute or otherwise insofar as permitted by Law.

28. CONFLICT OF INTEREST

28.1. The Recipient shall take appropriate steps to ensure that neither the Recipient, nor any employee, servant, agent or supplier, is placed in a position where there is or may be an actual conflict, or a potential conflict, between the pecuniary or personal interests of the Recipient, or such persons under the provisions of the Confirmation Document.

28.2. The Recipient will disclose to the Funder full particulars of any such conflict of interest which may arise. The provisions of this clause shall apply during the continuance of the Project and any period of Monitoring and Evaluation.

29. ANTI-CORRUPTION/BRIBERY

The Funder shall be entitled to terminate the Project and recover from the Recipient, the amount of any funding given if, at any time, it shall become known to the Funder that the Recipient has offered or given or agreed to give any inducement or reward to any person or company in relation to the obtaining of the funding or the execution of this Confirmation Document.

30. NOTICES

30.1. Any notice or other communication which is to be given by any Party to another Party shall be given by letter (sent by hand, post, Recorded Delivery or Special Delivery service), or electronic mail (confirmed in either case by letter).

30.2. Such letters shall be addressed to the other Parties at the addresses set out in this Confirmation Document. Provided the relevant communication is not returned as undelivered, the notice or communication shall be deemed to have been given two (2) working days after the day on which the letter was posted, or four (4) hours, in the case of electronic mail or sooner where the other Party acknowledges receipt of such letters, or item of electronic mail.

31. LAW

31.1. This Confirmation Document and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual

disputes or claims) are governed by, and construed in accordance with, the law of England.

31.2. The Parties irrevocably agree that the courts of England have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Confirmation Document or its subject matter or formation (including non-contractual disputes or claims).

SCHEDULE 1 - THE PROJECT

This project is to deliver domestic energy efficiency and low carbon retrofit activities within East Midlands Mayoral Combined Authority area. The Midlands Net Zero Hub (MNZH) is funded by the Department for Energy Security and Net Zero as part of the governments clean growth strategy and is hosted by Nottingham City Council. The project will be delivered by the Local Authorities in the region and reported through the MNZH.

The Local Authorities and Housing Associations with support from the MNZH are in the process of delivering three major retrofit programmes, Local Authority Delivery 2 (now concluded), Sustainable Warmth and Social Housing Decarbonisation Fund. The work supports the government's national commitment to reach Net Zero 2050 commitment.

Intervention is needed to help bridge the funding gap that currently exists where households who need support but are not receiving support due to the stringent criteria of the national funding schemes. The intervention will also better allow a place based approach enabling Local Authorities in the region to identify key areas of need, or fill in the gaps of existing programmes. Funds could also be utilised for additional measures in properties that further increases EPC rating and prevents repeat visits under future schemes minimising disruption and maximising benefits for the occupiers.

The funding is to be split equally amongst the 15 District and Borough Councils of the region and the 2 City Councils.

The objectives of the scheme are:

- 85 Whole House Retrofit approach scaled with all compliant required SAP measures installed (Target of 5 homes per LA)
- 600 PAS2035 compliant measures installed (Target of 36 per LA)
- Improved health and wellbeing for home occupier's through a pre and post survey
- Reduced consumption and lower carbon footprint
- Reduced number of households below an EPC C
- Average Standard Assessment Procedure (SAP) improvement

The scheme will also provide the following:

- To make further improvements on properties undergoing work through different schemes, reducing the need for repeat visits over a longer period of time. This is more cost and time efficient, and reduces interruptions to the households.
- To fill in the gaps where place based schemes are being rolled out at street and estate level, making sure properties within defined areas are not "left behind".
- To alleviate match funding pressures faced by other schemes.
- To enable properties to proceed that could not be supported through previous schemes due to rising material costs that exceed scheme cost cap.
- To enable a target, placed based approach.
- To demonstrate their ability to deliver successfully when provided with greater flexibility and control on the funding criteria.

Local Authorities are already in delivery mode, so this support will be an extension to work already ongoing and will offer Local Authorities the opportunity to return to households that have not aligned with current grant conditions, enabling a better service for citizens and giving the Local Authorities a greater chance to reduce fuel poverty in their areas.

A delivery plan for each LA demonstrating how they will reach their target within their allowance for each Local Authority will need to be provided by each LA prior to commencement of the work.

Appendix 1 to this Schedule comprises of the file entitled [Grant Conditions] which is embedded in the word version of this document and included in this document BELOW

APPENDIX 1 – GRANT CONDITIONS

SCHEDULE 2 - PAYMENT

1. TOTAL GRANT FUNDING

1.1. The total sum payable to the Recipient under this Confirmation Document is £583,500. This cannot be varied without the written consent of the Funder.

1.2. A funding schedule will be agreed for each Project and such evidence of eligible expenditure will be required on a monthly basis.

1.3. The eligible expenditure to date will need to be submitted by the Chief Financial Officer and verified as correct.

1.4. Only costs considered in line with the attached “Project costs”, identified in Schedule 1, should be included.

1.5. The Recipient will report immediately to the Funder any suspicions that funding has been overpaid, or that any financial mismanagement of the funding, or fraud, may have taken place.

1.6. For the purposes of this Confirmation Document, “financial year” shall mean the twelve month period, commencing on the 1st of April and ending on the 31st of March.

2. ELIGIBLE EXPENDITURE

2.1 The following items are **not** classed as eligible expenditure:

2.1.1 overheads allocated or apportioned at rates materially in excess of those used for any similar work carried out by the Parties;

2.1.2 notional expenditure;

2.1.3 payments for activity of a political nature;

2.1.4 depreciation, amortisation and impairment of assets purchased with the help of the Grant;

2.1.5 provisions;

2.1.6 contingent liabilities;

2.1.7 contingencies;

2.1.8 profit made by the Recipient;

2.1.9 dividends;

2.1.10 interest charges unless under an approved State Aid scheme;

2.1.11 service charges arising on finance leases, hire purchase and credit arrangements;

2.1.12 costs resulting from the deferral of payments to creditors;

2.1.13 costs involved in winding up a company;

2.1.14 payments for unfair dismissal;

2.1.15 payments into private pension schemes;

2.1.16 payments for un-funded pensions;

2.1.17 compensation for loss of office;

2.1.18 bad debts arising from loans to employees, proprietors, partners, directors, guarantors, shareholders or a person connected with any of these;

2.1.19 payments for gifts and donations;

2.1.20 entertainments;

2.1.21 reclaimable VAT;

2.1.22 statutory fines and penalties;

2.1.23 criminal fines and damages;

2.1.24 legal expenses in respect of litigation;

2.1.25 expenditure on activities of a political or exclusively religious nature;

2.1.26 expenditure supported from other government sources, local authority Grants, charges paid by leaseholders, or EU funding, to the extent that the combined Grants and other support total more than 100% of the Project or scheme costs;

2.1.27 expenditure on works or activities which any person has a statutory duty to undertake, except where there is strong justification in terms of the regeneration outputs or impacts that will result, e.g. in the case of beneficial activity brought forward, or carried out in a way which best promotes sustainable regeneration as a result of Grant support;

2.1.28 any liability arising out of negligence; or

2.1.29 payments made in advance of need.

3. OUTPUT PROFILE

3.1 Allocation of Grant is also subject to the Recipient having delivered the Outputs specified (if any) in accordance with the Targets and Output set out in Schedule 3.

3.2 The Recipient will need to complete, on a monthly basis, a return of Outputs delivered to date to enable the Funder to fulfil the Lead Funder's monitoring requirements to Department of Levelling Up, Housing and Communities (DLUHC) (or such equivalent government department from time to time).

3.3 In the event that the Recipient are unable to achieve the Output targets, then such Parties will notify the Funder as soon as possible and will use their best endeavours to reschedule delivery with the Funder's agreement, but the Lead Funder reserves the right to consider such an occurrence to be an Event of Default.

3.4 Not withstanding anything else set out in this Confirmation Document, the Funder may propose alternative monitoring requirements in the event that the Lead Funder is required to monitor grant funding in a different way by DLUHC or such equivalent government department from time to time). In such circumstances the Lead Funder shall vary this Confirmation Document in accordance with its terms.

4. GRANT PAYMENTS

4.1 The Recipient will receive its Grant allocation based on its monthly claim. The Recipient shall be required to complete the monitoring forms on a monthly basis

and provide an up to date monitoring report when required in accordance with Clause 3 above.

4.2 The Recipient will need to provide the Funder with bank details for the account in which it wishes the Grant to be paid into. This shall be provided to the Funder in letter format using the Recipients letter headed paper. They will also need to set themselves up on the Funders payment system.

4.3 Payment will be made within 30 working days of evidence of the payment date agreed

4.4 The grant profile below is based on the projects estimated expenditure profile as given in their business case. This will be updated in-line with the approved delivery plan.

	June	Sept	Dec	March 2024	Total
2023-24		£116,700	£203,300	£160,000	£583,500
2024-25	£103,500				

SCHEDULE 3 – KPI'S AND OUTPUTS

1. KEY PERFORMANCE INDICATORS – TARGETS AND OUTPUTS

1.1 The Recipient will deliver the Outputs as shown in the following Output Profile:

	Eligible homes signed up to receive measures-685		Whole Retrofits completed-85		Other measures installed*-600		Number of homes that improve to a EPC band C or above-411		Number of homes that have been improved by at least 1 EPC band from a starting SAP 1-54 rating (EPC-EFG)-170	
	Forecast	**Actual**	**Forecast**	**Actual**	**Forecast**	**Actual**	**Forecast**	**Actual**	**Forecast**	**Actual**
2023/24										
Q1										
Q2			0		0		6			
Q3	5		0		6		15			
Q4	36		0		15		15			
2024/25										
Q1			**5**		15		15			
Q2									36	
Q3										
Q4										

1.2 The Recipient must provide relevant evidence to support the output achievement.

SCHEDULE 4 – PROJECT TIME PLAN

1.1 The Recipient will complete the project as set out in schedule 1 of this document

2023/24	Key milestones from the Business Case e.g. Planning Permission granted, work commences on site etc.
Quarter 1	
Quarter 2	
Quarter 3	All homes signed up to receive measures. Whole Retrofit work begins Other measures work begins
Quarter 4	Whole Retrofit work complete
2024/25	
Quarter 1	Whole Retrofit work complete
Quarter 2	Other measures work complete
Quarter 3	
Quarter 4	

SCHEDULE 5 MONITORING AND EVALUATION REQUIREMENTS

1. Monitoring

1.1 The Project will be monitored until all outputs are achieved.

1.2 The Recipient is required to provide to the Funder a monthly report; the reports are to be provided by completing the Monitoring Form.

1.3 The Recipient may be subject to monitoring visits by the Funder on a routine basis and in the event of any queries arising

1.4 The Recipient will keep a record of all capital assets purchased using the Project funding and will retain the record for a period of seven years after the final payment or closure of the Project.

1.5 The Recipient shall permit officers (who have been duly authorised by the Funder in writing) such reasonable access to its employees, agents, premises, facilities and records, for the purpose of discussing, monitoring and evaluating the Recipient's (and any consultant or sub-contractors') performance of their obligations under this Confirmation Document and shall, if so required, provide appropriate oral or written explanations of them.

1.6 The Recipient will promptly provide all reasonable assistance required by the, Lead Funder, DLUHC (or such other equivalent government department from time to time), the National Audit Office, to monitor, review and verify compliance

by the Recipient with its obligations in this Confirmation Document, including reasonable access to its premises, documents and records for this purpose.

2. Evaluation

2.1 Projects will be evaluated at the end of the DLUHC spend period or the end of the project . A proforma report will be provided at the time. For this reason the Recipient will:

2.1.1 retain all original documents relating to the implementation of the Project and its costs for seven years after payment of the final amount of funding;

2.1.2 co-operate in respect of evaluation visits by, the Funder, or any other such party that the Funder have appointed, during the time in which Outputs are required;.

2.1.3 make staff available for interview if requested.

SCHEDULE 6 – INFORMATION SHARING AGREEMENT

Error! Reference source not found.6 to this agreement comprises of the file entitled (Information Sharing Agreement - XXXXXXXXX) containing the Information Sharing Agreement which is (i) embedded in the word version of this document BELOW.*

**At this stage an ISA is not anticipated to be a requirement as the reporting does not require personal data to be included. This schedule will remain dormant unless there is a change in reporting requirements from the Funder at which point a variation will be completed and this schedule will be updated accordingly.*

Signed for and on behalf of Nottingham City Council **as the Funder**	_____ **Colin Parr , Director** **Date:**
Signed for and on behalf of The Recipient by its duly authorised representative	_____ **Print Name:** _____ **Position:** _____ **Date:**_____

APPENDIX 1: MONITORING FORMS

Project Name	
Sponsor Name	
Monitoring Period	
Contact Name for queries	Name: Tel: Email:

Monitoring Forms

To be completed within 10 working days of the end of the month

	Eligible homes signed up to receive measures-685		Whole Retrofits completed-85		Other measures installed*-600		Number of homes that improve to a EPC band C or above-411		Number of homes that have been improved by at least 1 EPC band from a starting SAP 1-54 rating (EPC-EFG)-170	
	Forecast	Actual	Forecast	Actual	Forecast	Actual	Forecast	Actual	Forecast	Actual
2023/24										
Q1										
Q2			0		0		0			
Q3	36		0		6		6			
Q4			0		15		15			
2024/25										
Q1			**5**		15		20			
Q2									36	
Q3										
Q4										

Project Progress against Delivery Plan

Project milestones and outputs have been agreed at the project outset in your project delivery plan (as set out in Schedules 5).

Progress against these milestones will need to be reviewed regularly with the monitoring officer. Progress updates are required quarterly in the following format for milestones, outputs and expenditure.

If a milestone or output slips into a future quarter or year, it needs to be recorded as delayed and highlighted in the new quarter/year in which it has slipped to. This delay, the reasons behind it and mitigating actions need to be discussed with the monitoring officer and should be reflected in the project risk summary report if the delay will result in greater risk to the project. There should be a more detailed set of milestones and deliverables set out for the current financial year in question.

2023/24	Key milestones/deliverables from delivery plan scheduled to be achieved	Status (achieved or delayed)
Q1		
Q2		
Q3	All homes signed up to receive measures. Whole Retrofit work begins Other measures work begins	
Q4		
2024/25		
Q1	Whole Retrofit work complete	
Q2	Other measures work complete	
Q3		
Q4		

Quarterly Expenditure Monitoring Form

Date Paid	Suppliers Name	Invoice no.	Description of goods/services	Invoice total £ (net)	VAT £	Total inc VAT £ (gross)
TOTAL						

Narrative – Milestones and/or Outputs Achieved

I. Please provide an explanation for delays in the delivery of milestones/outputs that were due to this period
II. Is there any slippage anticipated for future milestones/outputs?
III. How will any slippage be corrected so that the agreed project timeline and expenditure profiles are not affected?

Please set out your responses to the questions above.

Issues

Please record any live critical issues with the project that require resolution. You should ensure that these are discussed with the monitoring officer for your project. These should include specific issues that affect expenditure and the delivery of the outputs as detailed in the other part of the monitoring report.

Summary report of significant issues

Description of Issue (include date raised)	Severity of issue.	Actions being taken and progress being made.

Add extra columns if applicable.

Future Changes to the Project

Have there been, or is there likely to be, any significant changes from the details given in your original application?

Yes ☐ **No** ☐

Please give details of these changes

Notes	
The provisions in the Grant Offer Letter relating to the Freedom of Information Act 2000 and the Data Protection Act 2018 apply to the contents of this return when completed.	
You are reminded that:	
(i)	you must notify us immediately if the circumstances of the Project change. (This refers particularly to any of the events listed in the Grant Offer Letter Schedule which deals with "Withholding and Repayment of Grant")
I certify that to the best of my knowledge and belief:	
1)	The information in this form is true and correct.
2)	At the time of this return I reasonably believe that the Outputs set out in the agreed and signed grant offer letter will be met.
Section 151 Officer/Finance Director's Signature	**Name (block capitals):**
Date	

REPORT TO:	**FINANCE AND MANAGEMENT COMMITTEE**	**AGENDA ITEM: 09**
DATE OF MEETING:	**05 OCTOBER 2023**	**CATEGORY: DELEGATED**
REPORT FROM:	**MONITORING OFFICER**	**OPEN DOC:**
MEMBERS' CONTACT POINT:	**ANTHONY BAXTER (EXT. 5712)**	
SUBJECT:	**MEMBER ICT PROTOCOL**	
WARD (S) AFFECTED:	**ALL**	**TERMS OF REFERENCE: G**

1.0 Recommendations

1.1 That the Committee reviews the refreshed member ICT protocol and recommends it to Full Council for approval.

2.0 Purpose of the Report

2.1 To review and recommend to Council for approval the refreshed member ICT protocol. To raise awareness of the newly created GDPR Handbook for elected members.

3.0 Detail

3.1 The current Member ICT Protocol is outdated. A new version has been drafted to refresh operational inconsistencies and reflect modern working practices. The protocol has been reviewed to ensure it aligns with responsibilities outlined in the Data Protection Act 2018 and guidance from the Information Commissioners Office (ICO).

The main changes to the document are listed below;

- Description on roles and clarification on when the ICT Protocol applies including clarification of responsibilities when using non-council devices and email addresses for Elected Members conducting casework.
- Additional of Identity Management section, including offer for corporate smartphone to all Elected Members.
- General updates renaming legacy software.
- Updated guidance on working practices such as the use of equipment in meetings, process in emergency situations and printing procedures.
- Updated appendix A in line with the current corporate security profile

- Updated appendix B to reflect their nature as guidelines for use.
- Included a new appendix C to provide information security classification.
- Removal of appendix D 'cover sheet' for signing.

3.2 The changes to the protocol have been informed by feedback from Elected Members. A cross-party working group reviewed the initial draft of the protocol and convened to discuss their findings. As a result, additional clarity has been provided regarding roles and responsibilities in relation to data controllers, personal use and data deletion. Where possible content has been streamlined and the group were also able to ask questions to the Head of Business Change and ICT about the meaning or inclusion of certain working practices. The group provided a very useful and productive assessment of the protocol and have been a welcome addition to the development of a Member document.

3.3 Introduction of corporate smartphones is a notable change. Elected Members will be able to request a corporate smartphone to access their SDDC emails, MS Teams, OneDrive, SharePoint Intranet and Identity Management. A personal device can be used for identity management if preferred, however the other functions will only be available on the corporate smartphone.

3.4 The new protocol also provides clarity on what IT and Data Protection working practices are relevant for each of the three roles performed by an Elected Member. These roles are also documented in the newly composed GDPR Handbook which is an information document to support training and development.

3.5 Appendix A (Password composition) represents best practice guidelines and should followed at all times, though it is recognised that some systems may be unable to support some of the recommended guidelines, due to technical limitations. The guidelines are in place for account credentials that do not enforce a specific combination by default.

3.6 Appendix B (Internet and Email guidelines) represents advice and guidance for effective use of those technologies.

3.7 Appendix C (Information Classification) gives guidance on the categories of information used by His Majesty's Government and the Government Security Classifications Policy.

4.0 Financial and Implications

None directly.

5.0 Corporate Implications

5.1 Employment Implications

None directly.

5.2 Legal Implications

None directly.

5.3 Corporate Plan Implications

None directly.

5.4 Risk Impact

The member ICT Protocol outlines security measures and acceptable use of technology to reduce the risk of unauthorised access to Council networks and data.

6.0 Community Impact

6.1 Consultation

None required.

6.2 **Equality and Diversity Impact**

Not applicable in the context of the report.

6.3 Social Value Impact

Not applicable in the context of the report.

6.4 Environmental Sustainability

Not applicable in the context of the report.

PROTOCOL FOR THE USE OF INFORMATION TECHNOLOGY BY MEMBERS OF SOUTH DERBYSHIRE DISTRICT COUNCIL

Version: 2.2

Date: September 2023

Contents

Version Control

Version	Description of version	Effective Date
1.5	Updated to reflect new ICT equipment, member requirements and best practice	April 2018
2.1	Updated to reflect current working practices and guidance	May 2023
2.2	Updated to reflect feedback from cross-party working group	September 2013

Approvals

Approved by	Date

Associated Documentation

Description of Documentation
Elected Member Data Protection Handbook

1.0 Introduction

The SDDC Member ICT Protocol is a document to govern Member use of Information Technology and is not intended to restrict you in carrying out your normal Council activities.

This policy relates to the use of ICT equipment, software and communication network when undertaking official Council duties only.

South Derbyshire District Council provides Members with ICT equipment to reduce costs and improve productivity and digital adoption should be the primary channel of business, as it is with Officers.

The ICT Protocol, which follows, exists for a number of reasons, the most important of which are:-

- To protect the Authority and its Members from prosecution. This can involve Data Protection, software usage, security and virus issues.
- To protect the assets owned by the Authority. These assets include not only software and hardware but also data.
- To standardise the working environment. This will allow every computer to operate the same, wherever you are located.
- To streamline ICT equipment procedures, giving users a faster response to faults.
- To enable Members to carry out their duties safely and more effectively.

In order for access to be granted to the Councils ICT infrastructure a Member must understand and accept this protocol.

Any breach of the Protocol may amount to a breach of the Members' Code of Conduct. In addition, any breach could lead to the equipment being recovered by the Council.

If you require clarification of any issue about the use of ICT, please contact ICT Services on 01283 387500, who will be more than happy to assist.

The Protocol will be monitored and reviewed periodically to consider any appropriate amendments necessary.

All other South Derbyshire District Council District Council codes, guidelines and policies apply in addition to the ICT Protocol

2.0 The role of the Member

1) They will act as a member of the Council undertaking official council business, for example, as member of a committee or sub-committee. As defined in the Code of Conduct a "Councillor" means a member or co-opted member of a local authority or a directly elected mayor. A "co-opted member" is defined in the Localism Act 2011 Section 27(4) as "a person who is not a member of the authority but who
(a) is a member of any committee or sub-committee of the authority, or;
(b) is a member of, and represents the authority on, any joint committee or joint sub committee of the authority;

2) They will represent the residents of their ward, for example, when undertaking casework.

3) They will represent a political party, particularly at election time.

Members will process personal data for different purposes depending on which of the above roles they are undertaking. This policy only applies when the elected member acting in the capacity outlined in point one above.

Who is accountable for the personal data, and therefore what devices and communication channels to use, when undertaking these roles?

Official Council duties
When a Member collects, uses and stores personal data when undertaking official Council duties such as attending a Committee, the Council is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Council will do this by providing Members with training, awareness, policies, procedures and guidance so that they know how to handle personal data properly and lawfully.

Undertaking Casework
When a Member collects, uses and stores personal data when undertaking casework, the Member is the Data Controller. The Member is accountable for the data they process as they will determine the means and purpose of processing and must ensure that it is used in the right way. If the Member chooses to use ICT equipment provided by SDDC for their casework they remain the data controller for the lifecycle of the data, however the Council will also be a data controller for data stored on our network and as such will secure its network to prevent data loss. If data breach has occurred from a data loss relating to SDDC networks the Council will report the incident to the ICO

It is assumed by the Council that Elected Members undertaking casework are responsible for knowing and abiding by the data protection principles.

Representing a Political Party
When representing a political party, for example when campaigning at election time, the political party is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Political Party may do this by providing its Members with appropriate training, awareness, policies, procedures and guidance.

Segregation of Duties & Personal Data

Data protection legislation requires that you have a very clear specified purpose for collecting and using personal data.

Once collected for a specific purpose, personal data cannot generally be used for any other purpose unless:

- the new purpose is compatible with the original, (or)
- you get the consent of the individual to use their data for another purpose,(or)
- you are required to use the information in another way by law (e.g. reporting a safeguarding concern).

For Members, the purpose for processing the personal data is linked directly to the role they are undertaking. For example, when representing a constituent, any personal data collected and used is for the specific purpose of dealing with the enquiry or complaint, and must not be used for any other purpose, e.g. political campaigning.

It is therefore important that Members segregate any personal data held for different purposes and roles.

As a Member of the Council

- Councillors may have access to, and process, personal information in the same way as employees e.g. Committee Reports. In this case it is the Council rather than the Councillor that is the Data Controller.
- Council is responsible for ensuring compliance.
- Data Breaches Must be reported to the Councils DPO within 72 Hours.

As a representative of the residents of their ward (Casework)

- When Councillors represent residents of their ward, they are processing personal information in their own right. E.g. using personal information to timetable a surgery appointment or take forward complaints made by local residents.
- It is the Councillor rather than the Council that is the Data Controller.
- The Councillor is responsible for ensuring compliance and reporting any data breaches to the ICO unless the data breach has occurred from a data loss relating to SDDC networks in which case the Council will report the incident to the ICO

As a representative of a political party

- When acting on behalf of a political party, for instance as an office holder, Councillors are entitled to rely upon the registration made by the party to determine how and why personal information is used. It is the Party rather than the Councillor that is the Data Controller.
- The Party is responsible for ensuring compliance. Data breaches should be reported to the Parties DPO.
- If a prospective Councillor is not part of a political party but campaigning to be an independent councillor for a particular ward, the candidate is the Data Controller.

2.0 Access to Authority ICT Systems

This policy relates to the use of ICT equipment, software and communication network when undertaking official Council duties.

In order to gain access to the SDDC systems, such as outlook, OneDrive, SharePoint and exempt information in CMIS it is necessary to have a valid username and password. Your username and password, also known as credentials, will be provided by a representative of ICT.

The password generated and assigned to a user account will follow strict protocol on its composition as documented later in this protocol and recommended by the National Cyber Security Centre.

Access to the Council's network away from Council buildings can only be gained through the use of Virtual Private Network (VPN). In order to access the VPN, users must authenticate through Multi Factor Authentication (MFA). The process of MFA involves a secondary device which a code or prompt can be sent to validate identity. This process is called Identity Management.

Members can choose to have a corporate smartphone to conduct this process or can use their personal device if preferred. Members are encouraged to request a corporate smartphone as this gives secure access to Council services, such as emails, documents and the intranet from any location.

No official council business is conducted through Identity Management and it is recognised that use of a personal device to conduct this is a choice of flexibility and does not amount to using a personal device to conduct official council business.

Your password will need to be changed upon first logon, equally there will be specific requirements as to the composition of your chosen password for security purposes. The password (Active Directory) will need to be changed every 60 days.

Any equipment provided by the Council must not be used for illegal purposes or in any way which could bring the Council into disrepute and must not be used to operate a private business.

The Council Member must not allow any unauthorised person to access the Council's systems using their network credentials or equipment and must keep all passwords secure. For more information on good practice on password control, please refer to Appendix A.

It should be noted that anything stored locally on Council equipment, explicitly, not on the network drives or OneDrive is not backed up by the Council. Members must only save documents to their U drive or OneDrive. Saving files to the desktop is prohibited.

3.0 Hardware Issued by the Authority

All ICT equipment, applications and data belong to and remain the property of the Council.

ICT equipment will be expected to be used for all democratic work, including use at Council meetings and reading/annotating agendas, reports, minutes and accessing SDDC emails.

The Member will take all reasonable steps to ensure ICT equipment is kept secure and protected from theft/damage. Particular care should be taken with regard to ensure ICT equipment is not left on view in cars or on public transport etc.

The Member will grant access to ICT equipment to any authorised employee or agent of the Council at reasonable times for the purpose of service, repair or audit.

If a Member ceases to be a Member of the Council, all equipment must be returned to the Council within 10 working days.

The storage or processing of personal data (e.g. details of names and addresses) may be unlawful in certain circumstances, advice is available from the Data Protection Officer or the Elected Member Data Protection Handbook.

Malfunctions with the ICT equipment should be reported to the ICT Service desk on 01283 387500. Under no circumstances should arrangements be organised for third party repairs to be undertaken.

Members should only use the following number to report or seek help for technical issues (01283 387500). This number is monitored continuously through operating hours. Members should not contact any officer on another number unless they have arranged this separately. This is in place to ensure Members receive a standardised and auditable service on each interaction.

In the event of damage to any part of the equipment, you should inform the ICT Service Desk immediately on (01283 387500).

In the event of theft or loss of ICT equipment the Member must report the incident to the Police to obtain a crime reference\lost property number and then provide this information to the ICT Service Desk on (01283 387500).

In respect of hardware issued for external connection to the Authority, the Council will insure and keep insured the hardware concerned.

In the event of the installed virus protection software discovering a virus on the hardware, you should follow the virus procedure as laid out below:-

Reporting the Action on Finding a Virus

- If a Member suspects a virus is affecting the operation of software and/or hardware, they shall switch off the hardware affected. Phone the ICT Service Desk immediately, who will advise what action to take.
- Do not try to ignore the fact that a virus may be affecting your files – it will not clear itself and will continue to infect other software files/hardware, and potentially other users of the network.

4.0 Internet Usage and External E-Mail

Any Member accessing the Internet for search/browsing or e-mail must ensure they adhere to the following rules:

- Do not access any websites that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council. Websites visited by any user (Member or officer) when connected to the Council server are recorded, monitored and will be available for audit, if necessary.

- If you accidentally enter any area which could be construed as unfit, obscene or inappropriate you must leave it immediately and inform the ICT Service Desk. Be aware that your computer records which sites you have accessed.

- Care must be taken when downloading files via the Internet. Computer viruses may be contained in files and/or e-mails and can severely damage the operation of the laptop. If the installed virus protection software detects any viruses, please follow the instructions on the previous page.

- If you receive unsolicited e-mail (e.g. junk or chain mail), do not forward such items to other recipients.
- Never leave the computer unattended whilst you are using the Internet. The session will be your responsibility. It should also be noted, the computer should not be left switched on and unattended for security purposes.

- E-mail guidelines and Internet guidelines are attached at Appendices B and C respectively.

5.0 Use and Care of the Equipment

All ICT equipment and system access supplied to you is primarily for your use relating to official Council duties.

Examples include:-

- Communicating with officers, other Members, MPs, government officials, partner organisations and where appropriate members of the public.
- Dealing with official Council correspondence.
- Communicating and obtaining information in support of approved personal training and development activities.
- Viewing and obtaining material for discussion by a political group on the Council, as long as that relates to the work of the Council and not the political party.
- Formulating policy and the decision-making process of the Council or other organisation on which you have been formally appointed to represent the Council.

5.1 Use for Party Political Purposes/Party Political Publicity

Under the Members' Code of Conduct, there is an absolute restriction on Members using, or authorising the use by others, the resources of the Council ('resources' includes land, premises and any equipment such as PCs, laptops, copiers, scanners, printers, paper and software and the time, skills and help of anyone employed by the Council) for political purposes.

There is also a clear statutory ban on the use of Council property for any purpose connected with party political publicity, either at election time or at any other time. Publicity is defined as any communication, in whatever form, addressed to the public at large or to a section of the public. This will include press releases and letters to the media.

At election time there are also detailed restrictions on the use of Council property for other party political purposes as well as publicity. The safest course is to avoid the use of Council ICT equipment for any purely party political purpose at any time.

This includes all the work you do in connection with:-

- Constituency party meetings, Ward party meetings etc. or communications to party members collectively in their capacity as party members.
- Processing names and addresses of your constituents for electioneering purposes.

5.2 Personal and Casework Use.

As explained in section 2 of this policy, Members typically have three roles. It is important to distinguish between these roles to ensure compliance with Council policy. It is strongly recommended when undertaking casework to use @southderbyshire.gov.uk communication channel and corporate device.

Members are permitted to communicate with the Council in relation to their casework on personal email addresses however it must be noted the risk for data in transit and the sharing of data collected in this capacity is the responsibility of the Member not the Council.

If a Member uses personal email accounts to conduct casework they are the sole data controller and will be responsible for reporting any data incidents to the ICO. If a Member uses their @southderbyshire.gov.uk email account the Council will at that point become an independent data controller with responsibility to keep data collected by the Member safe on the Council's network.

The use of personal email addresses (or third party addresses such as a work account) is strictly prohibited in relation to the sharing or discussion of internal affairs, such as confidential information, Council documents or any communication not intended for the public domain and you should use your South Derbyshire email account as your primary channel for these purposes.

The ICT equipment or services may be used for personal or casework purposes provided that:-

- It is not detrimental to corporate interests
- It does not cause any disruption, disturbance, inconvenience or degradation of the service
- It does not interfere with the work of the Council
- It does not involve unacceptable use of the Council's system
- The setup of the equipment and connection is not changed in any way

5.3 Examples of unacceptable use

- Breach of confidentiality
- Breach of security rules/guidelines, e.g. breaking through security controls
- Representing values which are contrary to any Council policy
- Promoting any private or personal interests such as selling personal possessions, property or promoting a social activity not related to the Council
- Deliberate accessing or attempting to access, viewing, downloading, displaying, printing or distributing from the internet of what is considered to be material likely to incite criminal behaviour
- Using or transmitting abusive, defamatory, libellous, profane or offensive language
- The importation of computer viruses and similar software through unauthorised downloading of files and programmes from external sources
- Running software that is not approved by the Council
- Loading software applications directly onto any of the Council's systems without approval
- Knowingly causing congestion and disruption of networks and systems
- Deliberate accessing or attempting to access, viewing, downloading, displaying, printing or distributing of what is considered to be offensive, obscene, sexually explicit or pornographic from the internet
- Sending e-mail messages and/or attachments that cause offence or are considered to be harassment on the grounds of gender, race, ethnic or national origin, disability, family status, age, religious belief, class or sexuality. Examples are messages that contain sexual innuendoes, racially biased jokes or obscene language.
- Using mobile data cards for personal use
- The use of proxy sites.

This is not an exhaustive list.

5.4 Monitoring of Communications

You need to be aware that the Council has the capability to monitor all use of the internet and intranet and logs and retains the records.

The reason that monitoring takes place is to ensure that the standards and rules set by the Council and legislation are complied with. This is also in place in relation to managing data security incidents.

We record or monitor:-

- Details of websites visited or attempted to be visited
- Pages accessed
- Files downloaded
- Graphic images examined
- Any file attachments (e.g. pictures or word documents)

The Council has the capability to monitor, log and retain e-mail correspondence.

Any potential viruses within e-mail and internet traffic passing through or outside the Council's systems are scanned for.

5.5 General Issues

Any messages or information you send to someone outside the Council, or statements that reflect on the Council (this is either in a personal capacity or on business use through an electronic network such as on-line services or the internet) wherever appropriate you must make it clear that the views expressed are personal and may not necessarily reflect those of South Derbyshire District Council.

You must not use anonymous mailing services to conceal your identity when mailing through the internet, falsify e-mails to make them appear to originate from someone else.

5.6 Care of the Equipment

Members are required to take all reasonable care of the Authority's equipment. Members should not eat, drink or smoke over the equipment.

Lending ICT equipment to any third party is strictly forbidden

Members should never attempt to delete software packages from ICT equipment. It should be noted that these will be updated or changed over time and ICT can do this remotely.

Members can only connect their ICT equipment to their home or third party Wi-Fi networks when using the Corporate VPN.

Do not subject the ICT equipment to extreme heat, cold or moisture (do not store in vehicles).

When carrying ICT equipment in a vehicle or on public transport every effort should be made to keep the device secure i.e. do not leave on display.

The whereabouts of the ICT equipment should be known at all times. It is the users responsibility to keep their equipment safe and secure.

One charger will be issued with each item of ICT equipment. If lost Members will be expected to replace these at their own cost.

5.7 Strictly forbidden Activity

Illegal installation transmission of copyright materials.

Members are not allowed to send, access, upload, download, or distribute offensive, profane, threatening, pornographic, obscene, or sexually explicit materials. Downloading other browsers is not permitted. Proxy sites are also prohibited.

Use of South Derbyshire District Council District Council's internet/E-mail accounts for financial or commercial gain or for any illegal activity.

5.8 Malfunction of Equipment

Malfunction or any other technical problem with ICT equipment should be reported to the ICT service desk 5705 (01283 387500), under no circumstances should repairs be organised without consultation with ICT.

5.9 Cameras

Members must use good judgement to ensure the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way.

If a Member would like to use a camera in meeting for photos or videos they should raise their intent with the meeting chair.

5.10 Social Media

ICT equipment provided to Members should not be used to access personal social media sites such as Facebook and Twitter. It is however permissible for Members to use equipment provided for social media for legitimate and official council business reasons such as communicating with residents or maintaining SDDC corporate sites. It is recommended that Members have separate social media accounts for personal and professional use.

5.11 Excessive Usage

ICT equipment cannot be used abroad without configuration changes. To use equipment abroad please contact the ICT service desk within 14 days of departure. Please note, to minimise security risk it is recommended not to use equipment abroad if the need isn't urgent or necessary.

Cellular data is provided to meet the business needs of the Council and appropriate usage tariffs will be selected accordingly.

The Council provides a mobile data contract which pools access to cellular network across the organisation. Each connection (sim card) is monitored for excessive use and proactive reporting is in place to stop any accidental connections incurring large overspends.

Wi-Fi connections should be used wherever possible to avoid additional usage charges. The Civic Offices (in Council Chamber & Members room) Wi-Fi will be preconfigured and equipment can easily be setup for home Wi-Fi or where this is provided in other locations such as Cafés, hotels. If assistance is required please contact ICT Services on 01283 387500.

5.12 Malicious Use/Vandalism

Any attempt to destroy hardware, software or data is forbidden. Defacing of ICT equipment, including the SDDC ID tag, in any way is prohibited (stickers, markers, etc.).

5.13 Printing

Members are only permitted to print out documents on the Council's network using a Council printer. These are located at Civic Office, Rosliston Forestry Centre, Oaklands and The Depot. This control is in place to safeguard against data loss through printing from the SDDC network to devices outside our network. Members can send a print job to a corporate printer via the laptop even if they are not at one of these locations. The job will only be released to print when the Member scans their badge on the top of the printer.

Members can also request Officers of the Council to print documents in relation to Committee meetings if they are unable to do so beforehand.

5.14 Microsoft Teams

The Council uses Microsoft Teams as its main collaboration tool. It is a communications tool which can also be used for joint working on documents and allows other collaborative functions such as task management.

Teams does not replace email in the case of formal communication of conducting business and a record of chat history is not kept. Members are encouraged to make use of Teams when contacting relevant and appropriate Officers as this in most cases is the fastest way to get a response given the complete integration of Teams in modern working practices.

5.15 Emergency Situations

In an emergency situation, the Chief Executive or other senior officer in the Council may issues an exemption to parts of this policy when responding to a major incident. This is likely to involve a balanced approach to risk and reward on any given situation and will be communicated widely at the relevant time.

6.0 The Law

6.1 Data Protection

All Officers and Members when conducting Council duties are responsible for complying with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 including any consequential data protection legislation as updated, amended or replaced from time to time which concerns the direct use of personal data, whether that information is held in electronic or paper-based form.

The Council has a statutory requirement to report Personal Data breaches to the Information Commissioners Office ("ICO") within 72 hours of becoming aware of the breach. Members must therefore report a breach (or any suspected breach) without undue delay to the Council's Monitoring Officer and Data Protection Officer. If the breach is likely to result in a high risk of adversely affecting the individual's right and freedoms, the Data Protection Officer will inform the individual.

The GDPR applies to Personal Data, meaning any information relating to an identifiable person who can be directly or indirectly identified, such as the name, identification number, location data or online identifier. It also applies to sensitive personal data such as genetic data and biometric data. For more information around Data Protection, please see the Elected Members Data Protection Handbook.

You should ensure that the Personal Data held for Council purposes should not be used for political purposes.

You should be aware that the unauthorised processing or disclosure of such data is prohibited under the GDPR, you are responsible for ensuring that there is no such unauthorised disclosure of data. If the Council fails to abide by the GDPR, it could be prosecuted and fined up to 20 million Euros (17 million pounds) or up to 4 per cent of the Council's turnover. The GDPR also imposes legal liability if you are responsible for a breach. In addition, the Council or the individual officers may be liable to pay compensation to any individual who has suffered material or non-material damage as a result of such a breach.

6.2 Computer Misuse

The Computer Misuse Act 1990 covers unauthorised or malicious use of any computer system. It is the law used to prosecute hackers and people who write and distribute computer viruses deliberately.

It is a criminal offence to access, or attempt to access, any computer system you are not authorised to access. This law protects against employees and members of the public who deliberately cause damage to systems and data. The Act also makes it illegal for a person to deliberately delete data or sabotage systems to the detriment of the Council.

6.3 Harassment

You can commit harassment either by using e-mail or send a harassing message to someone or by downloading and distributing material from the Internet which constitutes harassment because it creates an intimidatory working environment. Harassment and discrimination are unlawful under the Protection from Harassment Act 1997 and the Equality Act 2000. As with any form of harassment under the anti-discrimination legislation, the intention of the parties is irrelevant. The problem with e-mail is that, with the lack of visual clues, offence may be caused where none was intended.

6.4 Obscene Material

Publishing legally 'obscene' material is a criminal offence under the Obscene Publications Acts 1959 and 1964. This includes electronic storing and/or transmitting obscene materials that would tend to deprave and corrupt or paedophiliac material.

6.5 Defamation or false statements

The liability for defamation or false statements applies to electronic communication just as it does to more traditional forms of communication. Anyone who e-mails a libellous or false e-mail message or posts such a message on the Internet will be responsible for it and liable for any damage in accordance with the Defamation Act 2013 for causing or likely to cause serious harm to the reputation of the victim.

In addition to the liability of the individual who made the libellous or false statement, the Council may also be held liable. This could be either under the normal principles of:-

- Indirect liability because the Council is considered responsible - known as 'vicarious liability'; or
- Direct liability as a publisher because of providing the link to the Internet and e-mail system.

An untrue statement that damages the reputation of a person or company by causing people to think worse of them will generally be defamatory. Similarly, a false statement intended to cause damage to a person or their economic interests can bring a claim for damages.

Do not put anything on an e-mail or an attachment, which you would not put in a normal letter on Council headed paper. Treat e-mail as you would a postcard going through the open post.

6.6 Copyright

Although any material placed on the Internet or in public discussion areas is generally available, the originator still has moral and, possibly, legal rights over it. You should not copy it without acknowledging the original source and, where appropriate, gaining their permission. This applies even if you modify the content to some extent. Please note that any official material placed on a website is subject to copyright laws.

Copyright laws are different for each piece of software. In general, the copyright to every piece of software run on a system is owned by whichever company or person wrote it. The Council has a legal duty to make sure sufficient licences of the correct type are present to cover the use of all software. You must be aware of these issues and make sure that the Council has correct licences for any software you are using.

6.7 Contracts

Electronic communication, such as e-mail, is generally regarded as an informal means of communication but it is, nevertheless, capable of creating or varying a contract in just the same way as a written letter. You should be careful not to create or vary a contract accidentally, always seek advice from the Legal department if you believe you are being requested to act on behalf of the Council and sign an electronic document.

6.8 Disclaimer

Despite putting confidential disclaimers and, where appropriate, personal disclaimers, on external communications, there is still nevertheless a legal connection to the Council. Always remember that any statement you make may still be construed as representing the Council.

7. Responsibilities

Violation of the Acceptable Use Policy may be subject to but not limited to; action under the Member Code of Conduct, repossession, removal of content.

7.1 Member

Violation of the Member ICT Policy may be subject to but not limited to; action under the Member Code of Conduct, repossession, removal of content.

- All material viewed and stored on ICT Equipment must be in accordance with the ICT protocol and values of South Derbyshire District Council.
- Users must exercise the same prohibited uses as the use of South Derbyshire District Council computers, corporate mobile devices and laptops.

7.2 Corporate ICT

- Provide SDDC supplied ICT equipment to a recognised standard build that can access the Internet and SDDC emails from the users SDDC email account.
- Ensure any incidents in relation to ICT equipment acceptable use protocol are referred to Democratic Services and support with any investigation as necessary.
- Provide support and maintenance of ICT equipment in keeping with the corporate ICT service standards.
- Providing training and instruction on use of the SDDC estate.
- Providing advice and support to staff and Members regarding ICT equipment
- Investigation of any suspected misuse of devices
- Will be responsible for the deletion of any data, email accounts and files in line with current retention protocol when a Member leaves office. If a Member wishes to retain data they have collected for casework then a request can be made to the IT helpdesk.

APPENDIX A - PASSWORD COMPOSITION

Passwords for accessing systems should be of a complex nature.

The following guidelines give information on how passwords should be created and managed to ensure their integrity and the integrity of the systems and information, which they protect.

The following best practice guidelines should followed at all times, though it is recognised that some systems may be unable to support some of the recommended guidelines, due to technical limitations.

Password Requirements

To ensure that malicious parties or programs which guess passwords have reduced chance of being successful, users should construct a password that meets the minimum criteria for each system as shown in the table below.

System / Type	Password Age	Minimum requirements	Lockout / Wipe attempts
Network Accounts and Systems which can enforce password blacklists	60 Days	8 Characters	3
SmartPhones	60 Days	8	5 attempts and then the device wipes
Members	60 Days	8 Characters	3

To make sure the password is strong users should also ensure that passwords:

- must not contain the user login name
- must not include the user's own or relative's name, employee number, national insurance number, birth date, telephone number, car licence plate or any information about him or her that could be readily learned or guessed
- should not be single words from an English dictionary or a dictionary of another language, slang, dialect or jargon with which the user has familiarity. This is true even with a number placed at the end
- are significantly different from previous passwords and password used for other systems. Do not reuse old passwords or words spelt backwards
- do not contain commonly used proper names, including the name of any fictional character or place
- do not contain any simple pattern of letters or numbers such as "12345678" or "abc123", or deliberately misspelled words

- are not displayed in work areas or any other visible place. If a user has to write their password down, they must ensure it is kept as securely as, for example, their credit card. Write down only the password, not the system it is for and if possible include a mistake. Inform ICT should this go missing
- are not e-mailed, recorded electronically, or used via the “save password” functionality which may result in a password being taken or shared
- Finally, be careful when using systems which allow users to enter a password reminder or hint; the reminder or hint must not be the user’s name, password or text which clearly identifies the password (e.g. child’s name) as this is a security risk, and users MUST NOT let anyone observe them when entering their password.

Password Changes

Network passwords must be used in line with the following rules:

- Passwords must be changed when a new account is created
- Passwords must be changed, as soon as possible, after a password has been compromised or after a suspected compromise
- Passwords must be changed where they are deemed to be too weak
- Passwords must be changed on direction from the Council’s ICT staff
- Passwords are changed and the account deactivated when the staff member leaves the Council
- Administrator passwords should be changed whenever a member of staff leaves the Council who had administrator access.

Password Suspension

The network will permit three attempts to enter the correct User ID and password before the account is locked. Smartphones and tablets allow five attempts before wiping the device.

When an account has been suspended, it can be released by the appropriate system administrator. In the case of the network (log on) or systems managed by ICT requests for release of suspended accounts should be made via the IT Service Desk.

To reset a password for individual applications, the relevant System Owner for that system should be contacted.

Password and Account Protection

Each user is responsible for all activities originating from any of his or her username(s).

Passwords must not be shared. Users who share their passwords may have their access to the Council’s networks and systems disabled, whilst investigations are carried out and management determine the course of action (disciplinary) that may be required.

NOTE: In some cases, users may be requested to share their passwords with trusted Council employee (Audit, ICT Security, HR) in order to complete a task that is critical to the Council. In this case Director approval can be sought for an exception.

Avoid writing down passwords; if passwords are to be written down they **must** be protected. Do not stick them to the equipment they unlock or leave them out in desks, notice boards or any other place

where someone may see them. If a password must be written down, keep it securely in a wallet or purse or locked in a secure container. Ideally do not keep the corresponding username with the password as this will make it harder to use if it is lost. If possible, only record part of the password. Report lost password documentation **immediately** so that unauthorised access can be blocked.

Password Construction

Creating strong passwords does not have to be difficult, try this method.

What to do	Example
Start with a sentence or two	Longer passwords are better than short
Remove the spaces between the words	Longerpasswordsarebetterthanshort
Add shorthand and misspell words	LingerpswdsRsafethnsht
Add length with numbers and symbols, don't always do this at the start or end.	LingerpswdsRsafethnsht1876

While this password is fairly easy to remember the number of combinations an attacker would have to check is huge. Even if an attacker can check billions of passwords a second on thousands of computers it would still take too long to find the password.

APPENDIX B – EMAIL AND INTERNET GUIDELINES

These guidelines apply equally to internal and external e-mail and act as guideline.

Never . . .

1. Use the e-mail system for knowingly doing anything illegal under English law, or for unacceptable purposes that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council.

2. Transmit sensitive information on e-mail unless you can apply appropriate encryption using the 'sensitivity' button in Outlook.

3. Abuse others - even in response to abuse directed at you.

4. Use e-mail to harass or threaten others in any way.

5. Use anonymous mailing services to conceal your identity or falsify e-mails to make them appear to originate from someone else.

6. Access anyone else's mailbox unless they have given you proxy or authorisation rights. Unauthorised access is a breach of security.

Don't . . .

7. Use the 'Reply All' function unless everyone in the original message needs to know your response.

8. Print out messages unless you really need to.

9. Send large e-mails or attachments. It's not an economical or sensible way to handle large documents and it can halt the e-mail system. It is better to put the file on the network and direct people to it. Contact ICT for assistance.

10. Create e-mail congestion by sending trivial messages or by copying e-mails to those who don't need to see them.

11. Forward confidential or restricted items on e-mail sent to you personally without the originator's permission.

Remember . . .

12. E-mails may be read by a far wider audience than originally intended, because of the ease of forwarding messages to new recipients.

13. E-mail is not guaranteed to arrive at its destination within a particular time, or at all.

15. Always put appropriate disclaimers on your messages.

16. Any advice you give on e-mail has the same legal standing as any other written advice.

17. Before sending an e-mail, ask yourself how you would feel if your message were read out in Court or disclosed under FOI.

18. Not to assume that the message has been read just because it has been sent.

Do . . .

22. Maintain your e-mail mailbox properly:-

- Access emails regularly or make sure that a re-direction is set up if you are away for more than a day.
- Only keep messages that are necessary for current business needs or need to be retained for other purposes.
- Store all e-mail messages necessary for permanent business records in your U Drive or OneDrive, according to current record retention policies.
- Delete insignificant, obsolete and unnecessary messages, return/read receipts and attachments, regularly. Clear your 'deletion' folder daily to get rid of unwanted items.

23. Make sure you use the correct address when sending mail. If the e-mail fails to reach its destination, it may be lost or fall into the wrong hands. Double-check the address when you send important messages.

24. Consider confirmation of receipt for important e-mails.

25. Reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will or should be sent.

26. Only print an e-mail if you need to for example, a hard copy for filing / legal reasons.

28. Always enter a subject title to your e-mail. Make sure that the 'subject' field of the message is meaningful. This helps everyone file and search for his or her messages more effectively.

INTERNET GUIDELINES

If you use a connection to the Internet, you must follow the requirements of these guidelines.

Never . . .

1. Use the Council's Internet access for knowingly doing anything which is illegal under English law, or the law of any other relevant country, or for unacceptable purposes such as accessing any www area that could be construed as unfit, obscene or would otherwise be considered as inappropriate for a Member of the Council.

2. Use the Council's Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.

3. Knowingly use the Council's Internet facilities to disable or overload any computer system, network, or equipment or attempt to disable, defeat or circumvent any systems intended to protect the privacy or security of another user, including the Council's 'firewall' security systems.

Don't . . .

5. Leave Internet connections unattended.

6. Release protected information online - whether or not the release is inadvertent, it comes under all the penalties under existing data security policies and procedures.

7. Order or pay for personal goods and services using Council equipment on the Internet.

Remember . . .

8. If you accidentally access unsuitable material, you must disconnect from the site immediately and inform the senior officer in ICT Services.

Do . . .

9. Only use Internet browser software provided and configured by the Council, and only use officially provided access mechanisms.

10. Immediately report any security problems or breaches to the ICT Service Desk.

APPENDIX C – INFORMATION CLASSIFICATION

The Council's partnership working with Central Government and other national bodies and agencies has led to the exchange and sharing of information that requires protection and handling in line with the requirements of the Public Services Network and the Government Security Classifications Policy (GSCP). The GSCP describes how HM Government classifies information assets to: ensure they are appropriately protected; support Public Sector business and the effective exploitation of information; and meet the requirements of relevant legislation and international / bilateral agreements and obligations.

Organisations which work with government have a duty to respect the confidentiality and integrity of any HMG information and data that they access, and are accountable for safeguarding assets in line with the GSCP.

Purpose and principles

The purpose of this guidance is to ensure the Council meets its obligations under the GSCP and also has appropriate controls in place to protect its own information. It reflects the following principles:

Principle One: All information that the Council collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection.

Principle Two: Everyone who works with the Council (including staff, members, contractors and partners) has a duty of confidentiality and a responsibility to safeguard any Council information or data that they access, irrespective of whether it is marked or not, and is must be provided with appropriate training.

Principle Three: Access to sensitive information must be granted on the basis of a genuine "need to know" and subject to an appropriate personnel security control.

Principle Four: Assets received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

Classification / Categorisation of the Council's Information Assets

The GSCP classifies HMG information assets into three types: OFFICIAL, SECRET and TOP SECRET.

The Council operates exclusively at OFFICIAL level and the previous classifications, RESTRICTED, PROTECTED and UNCLASSIFIED no longer apply.

The main theme of the new Government policy is, at OFFICIAL at least, personal responsibility for the data you transmit, handle or store, no longer relying on security markings. This is particularly important because the UNCLASSIFED marking no longer exists.

OFFICIAL information

The OFFICIAL level covers the variety of information handled and created by the Council of differing value and sensitivity and different consequences resulting from loss of compromise.

Some of the Council's information is particularly sensitive and could have more damaging consequences (for individuals, the Council or partner) if it were lost, stolen or published in the media

This sensitive information will attract additional controls to ensure that it is only accessed by those with a "need to know". Such information should be treated as OFFICIAL–SENSITIVE.

Guidance on what information should be treated as OFFICIAL–SENSITIVE and how it should be handled appears below.

It is important to note that within the GSCP, CONFIDENTIAL is not a recognised security classification; therefore care must be taken if marking documents as confidential. It must be clear to the recipient of the information what this means and what handling requirements are to be applied.

Marking OFFICIAL information

There is no requirement to explicitly mark routine OFFICIAL information.

Security markings previously applied to council information which now fall in the OFFICIAL classification can therefore be removed.

Handling OFFICIAL information

All Council information must be:

- Handled with care to avoid loss, damage or inappropriate access.
- Shared responsibly, for business purposes, and using appropriately assured channels if required (e.g. Secure email).
- Stored securely when not in use. For example, with clear desk policies and screens locking when ICT is left unattended.
- Protected in transit and not left unattended when taken out of the office.
- Stored securely when taken out of the office. For example in a locked briefcase or locked cabinet.
- Protected to prevent overlooking or inadvertent access when working remotely or in public places.
- Discussed with appropriate discretion when in public or over the telephone. Details of sensitive material should be kept to a minimum.
- Emailed, faxed and sent by letter only to named recipients at known addresses.
- Destroyed in a way that makes access unlikely. More sensitive assets should be returned to the office for secure disposal where appropriate.

Special Instructions when handling personal data

The General Data Protection Regulations requires the Council to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk pf processing personal data.

Whilst personal data will generally fall in the OFFICIAL classification, additional controls must be observed to ensure that the Council complies with its obligations under the Data Protection Act.

- Original certificates (e.g. birth certificates, medical records, passports) should be transferred / returned by Tracked Courier;
- Multiple and restricted lists (e.g. names and addresses) should be sent by Tracked Courier and if held on electronic media, strong encryption should be used with a strong password (see Password Policy);
- Paper records containing personal data must be kept secure when off-site in a lockable case and totally separate from valuable items such as laptops;
- Partnership arrangements where electronic files of personal data are transferred should be by secure electronic methods only and encrypted except for Public Services Network.
- An individual's personal data may be sent by normal email where they have given the Council permission to send via this channel, else use secure email. The individual must also acknowledge that we cannot be held responsible if a 3rd party gains the information after the Council has sent it;
- It is the senders responsibility to ensure that the recipient's email address is correct and the receiver is ready to handle the information being sent in the required format. Specific care must be taken to ensure that personal data is not sent to recipients on a contacts list;
- When printing personal data, check that all print jobs that start are completed. Where jobs cannot complete (e.g. owing to a printer error) ensure that they are deleted from the print queue. Failure to do this could result in the print job resuming in their absence, and result in personal data being left out on the printer;
- When printing personal data, the document must be removed from the printer immediately. Personal data must never be printed to a printer accessible to the public unless the secure print facility is used;
- All unwanted printed material containing personal data must be shredded.

For any advice please contact the Data Protection Officer or ICT Service Desk.

OFFICIAL-SENSITIVE information

OFFICIAL-SENSITIVE is not a separate classification; it is simply a tool to identify OFFICIAL information that is particularly sensitivity and needs additional controls.

OFFICIAL-SENSITIVE should be used by exception and in limited circumstances where there is a clear and justifiable reason to reinforce the “need to know." This would be when compromise or loss of the information could have particularly damaging consequences for an individual (or group of individuals), a partner, or the Council.

Some examples of OFFICIAL-SENSITIVE information are as follows:

- the most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to members on contentious and very sensitive issues;
- commercial information e.g. contract negotiations that may be damage/undermine the Council or commercial partner’s negotiating position if improperly accessed;
- information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- sensitive personal data;
- legal advice and information created in connection with legal proceedings.

Determining whether information is OFFICIAL-SENSITIVE

The originator of the information is responsible for determining the appropriate classification for any assets they create, with reference to this Policy, and marking the asset where OFFICIAL-SENSITIVE.

The originator must understand the business value and sensitivity of the information they create. Information should not be regarded as OFFICIAL-SENSITIVE as a matter of routine as applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls. However, not applying the OFFICIAL-SENSITIVE marking to sensitive assets may result in inappropriate controls and potentially put them at greater risk of compromise.

Responsibility for any change in the classification lies with the originator. Recipients must not re-classify a document without the agreement of the originator. Where that agreement cannot be obtained, for example because the originator no longer works for the Council, agreement must be obtained from the originator’s manager.

Marking OFFICIAL-SENSITIVE information

When sending emails where interception could compromise the freedoms of recipients or data subjects an additional level of security can be added to the email via Outlook. This action will mark the email as OFFICAL-SENSITIVE.

A user should click on the ‘Sensitivity’ button in a new message and selecting ‘Official -Sensitive’. Note, this will change how the email is received and will require the recipient to take an extra step in order to read the message.

For assistance on secure electronic transmission of files please contact the ICT service desk.

South Derbyshire District Council

Elected Member Data Protection Handbook V1.1 [Draft]

September 2023

Contents

Version Control

Version	Description of version	Effective Date
1.1	Adoption	

Approvals

Approved by	Date
Data Protection Officer	
Leadership Team	

Associated Documents

Name
SDDC Member IT Protocol

About this guidance

This guidance has been developed for Elected Members. It serves as a useful reference to support Members in complying with the requirements of data protection legislation by providing practical advice, information and guidance on the collection, use and storage of personal data.

The advice and guidance contained in this document is primarily aimed at Members when representing the Council. However, the guidance may also be adopted by Members when collecting and using personal data for the purpose of casework (should they wish to do so).

It is entirely up to Members to decide whether or not this guidance is adequate in this regard and to adopt it for casework purposes. Whilst this guidance mirrors the key topics and themes covered in the formal Data Protection training that is provided to Members, it should be noted that the guidance is not intended to replace this training, nor the advice that is available from the Data Protection Officer.

Glossary of Terms:

The following terms appear regularly throughout this document. Their definitions are below:

Official Council duties or Council Business: The work undertaken by a Member when representing the Council, for example attending or chairing a committee.

Casework: The work undertaken by a Member when representing a constituent. This may include a direct query, complaint, service request, community issue, etc.

Data protection legislation: Refers to current data protection legislation within the UK.

Data Controller: The individual or organisation that determines the purpose for which personal data is collected and used. The Controller is ultimately accountable for the personal data.

Processing: In relation to personal data, this can be any activity involving (but not limited to) the collection, use, storage, sharing, and disposal, etc. of the personal data.

Information handling principles

Data protection legislation sets out good information handling principles that Members must follow. The key principles are summarised below and are covered in more detail within this guide:

1. Keeping people informed

You must be open, honest and transparent with people about the way you use their personal data and provide them with appropriate privacy information.

2. Specified Purpose

You must collect and use personal data for a specified purpose and stick to that purpose.

3. Minimisation

You must only collect the personal data that it absolutely necessary in relation to the purpose.

4. Accuracy

You must take reasonable steps to ensure that personal data is correct and kept up-to- date where required.

5. Retention

You must not keep personal data for is longer than is needed in relation to the purpose.

6. Information Security

You must ensure that personal data is kept safe and secure.

7. Information Rights

You must ensure that people are made aware of their information rights and are able to exercise them.

1.0 How data protection applies to Members

This section aims to explain how data protection legislation applies to Members when collecting and using personal data when undertaking official Council duties, casework and when representing a political party.

The role of a Member

1) They will act as a member of the Council undertaking official council business, for example, as member of a committee or sub-committee. As defined in the Code of Conduct a "Councillor" means a member or co-opted member of a local authority or a directly elected mayor. A "co-opted member" is defined in the Localism Act 2011 Section 27(4) as "a person who is not a member of the authority but who
(a) is a member of any committee or sub-committee of the authority, or;
(b) is a member of, and represents the authority on, any joint committee or joint sub committee of the authority;

2) They will represent the residents of their ward, for example, when undertaking casework.

3) They will represent a political party, particularly at election time.

Members will process personal data for different purposes depending on which of the above roles they are undertaking. This policy only applies when the elected member acting in the capacity outlined in point one above.

Who is accountable for the personal data, and therefore what devices and communication channels to use, when undertaking these roles?

Official Council duties
When a Member collects, uses and stores personal data when undertaking official Council duties such as attending a Committee, the Council is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Council will do this by providing Members with training, awareness, policies, procedures and guidance so that they know how to handle personal data properly and lawfully.

Undertaking Casework
When a Member collects, uses and stores personal data when undertaking casework, the Member is the Data Controller. The Member is accountable for the data they process as they will determine the means and purpose of processing and must ensure that it is used in the right way. If the Member chooses to use ICT equipment provided by SDDC for their casework they remain the data controller for the lifecycle of the data, however the Council will also be a data controller for data stored on our network and as such will secure its network to prevent data loss. If data breach has occurred from a data loss relating to SDDC networks the Council will report the incident to the ICO

It is assumed by the Council that Elected Members undertaking casework are responsible for knowing and abiding by the data protection principles.

Representing a Political Party
When representing a political party, for example when campaigning at election time, the political party is the Data Controller and is accountable for ensuring that the data processed by the Member is used in the right way. The Political Party may do this by providing its Members with appropriate training, awareness, policies, procedures and guidance.

Segregation of Duties & Personal Data
Data protection legislation requires that you have a very clear specified purpose for collecting and using personal data.
Once collected for a specific purpose, personal data cannot generally be used for any other purpose unless:

- the new purpose is compatible with the original,

OR

- you get the consent of the individual to use their data for another purpose,

OR

- you are required to use the information in another way by law (e.g. reporting a safeguarding concern).

For Members, the purpose for processing the personal data is linked directly to the role they are undertaking. For example, when representing a constituent, any personal data collected and used is for the specific purpose of dealing with the enquiry or complaint, and must not be used for any other purpose, e.g. political campaigning.

It is therefore important that Members segregate any personal data held for different purposes and roles.

2.0 Keeping People Informed

This section explains what information a Data Controller (DC) must provide to individuals when you collect their personal data.

What data protection law requires
Data Protection law requires that Data Controller's are open and honest with people about the use of their personal data. This is especially important in situations where the individual has a clear choice about whether they wish to enter into a relationship with you (for example, where a constituent is considering asking you to represent them on a particular matter) or the use of their data may be unexpected.

When collecting personal data from an individual it's important to provide an explanation as to how their data will be used and for what purpose. By providing this information, individuals will know from the outset how their personal data will be used and the likely implications for them. This is likely to prevent complaints or concerns being received from individuals about the way you are using their personal data.

What information must I provide to individuals?
The law sets out what information must be provided to individuals when you collect their personal data. At a minimum, and as a starting point you must always tell them:

- Who you are;
- Why you need their information;
- What you are going to do with it;
- Who it will be shared with.

The information that DC's provide to individuals about the way their personal data will be used is often referred to as 'privacy information'. In written form it is referred to as a 'privacy notice'.

How and when should I provide privacy information to individuals?
Data protection law does not specify how privacy information should be provided to individuals. Good practice is to use a blended approach using a number of communication methods and techniques.

The following outlines how privacy information is/should be provided to individuals when you are representing the Council or undertaking casework.

2.1 Official Council duties

Who is responsible for providing individuals with privacy information?
In relation to the personal data you may process when undertaking official Council duties, it is the responsibility of the Council to ensure that citizens, service users, customers and visitors are informed about how the Council, via its Members and Officers use their personal data when providing them with services.

How does the Council provide individuals with privacy information?
The following outlines the key ways in which the Council provides privacy information to individuals. This is in addition to any verbal privacy information that officers may provide to individual when they make contact directly with the Council.

Main Privacy Notice
The main Privacy Notice is published on the Council's website under the Data Protection section. The notice consists of a series of webpages that provides individuals with information on the following topics:

- How we use your personal information – An Overview
- Introductory page about the way the Council uses personal data and the ways in which we protect people's privacy.
- How we use your personal information – frequently asked questions
- Answers to commonly asked questions about the Council's use of personal data.
- Your information rights
- Provides information on an individual's information rights and how they may be exercised.
- Concerns or complaints about the way the Council is handling your personal information Provides information on how an individual can raise a concern or make a complaint about the way the Council is handling their personal data.

Service Privacy Notice
Each Service has developed a more detailed privacy notice to compliment the main privacy notice. Service Privacy Notices are also published on the Council's website. They include specific information about what personal data each service collects, where the data comes from, who the data is shared with and how long it is kept for.

Forms and Applications
Forms and applications used to capture personal data from citizens, residents and applicants contain a short privacy statement that explains to individuals how the personal data requested on the form will be used by the Council. The statement also signposts individuals to the Council's website for more detailed information.

2.1 When undertaking casework.

Who is responsible for providing privacy information to constituents?

When undertaking casework, the Member (as the Data Controller) has a direct responsibility under data protection law to provide privacy information to constituents.

3.0 Casework - Authority to Act

This section provides guidance on whether a Member needs authority from an individual to represent them or to discuss their concern with an organisation.

Do I need written authority from a constituent to represent them?
Data protection law does not require a Member to have written authority from a constituent to represent them. However, some Members may prefer to have something in writing, particularly in situations where the query or concern is of a sensitive nature. That way there can be no doubt that the constituent has requested your assistance in resolving their concern.

For indirect enquiries, do I need the consent of the individual who the enquiry is about before I take on the casework?

Example: An indirect enquiry is usually referred to as an enquiry received from a third party on behalf of an individual. For example - a daughter acting on behalf of her frail elderly mother contacts you for support regarding her mother's benefit claim.

In the above example, you would need confirmation from the mother that she is happy for the daughter to act on her behalf. This could be achieved through a simple phone call to the mother.

If the mother is incapable of confirming this, for example, if she suffers with dementia and does not have capacity, you should request proof from the daughter that she has authority to act on her mother's behalf (e.g. proof of power of attorney, confirmation that her mother's finances are in her name (bank statement), etc.). This authority should not be assumed even if the individual is known to you.

Do I need to provide proof of authority to act when requesting information from an organisation?

When undertaking casework you may be required to contact organisations to assist you in resolving the enquiry or concern. These organisations may include (but are not limited to) services within the Council, Local Health Board, GP Practice, Job Centre, Department for Work and Pensions, etc.

Often, as part of that organisation's data protection procedures, especially where a Member is not known to the organisation, the organisation may ask you to provide proof that you have authority (sometimes referred to as consent) to act on the constituent's behalf. In addition, the organisation may ask you to confirm your identify as an Member.

This request for authority / proof should not be perceived as a barrier or the organisation being obtrusive, but good practice that ensures personal data is not discussed or disclosed to someone acting under a false pretence.

4.0 Data Quality

This section covers what is commonly referred to as the ‘data quality’ principles. It includes good practice, hints and tips relating to data minimisation, keeping personal data accurate and up-to-date and retention.

Data minimisation

Data protection law requires that:

a) You collect enough personal data to sufficiently fulfil the purpose for which the personal data is being processed;

b) The personal data is relevant to the purpose for which it is being collected; and

c) It is limited to what is necessary in relation to that purpose.

Here are some hints and tips to help you comply with this requirement when undertaking casework:

- Ensure you have a clear reason for collecting and holding the personal data and can justify this if challenged.
- Collect and hold no more data than you need – always the minimum amount.
- Don’t collect or hold personal data “just in case” it might be needed.
- Consider each enquiry on a case by case basis and carefully decide what personal data you need to resolve that particular enquiry.
- Look for alternatives – do you need someone’s date of birth or is their age enough?
- If you’ve collected personal data that you didn’t actually need, delete it.

Accurate & Up-to-date

- You must take reasonable steps to ensure the accuracy of the personal data that you collect and record.
- You should consider whether the personal data you collect and record needs to be kept up-to-date.
- If you discover that the personal data is incorrect or misleading, you must take reasonable steps to correct or erase the personal data as soon as possible.

Here are some hints and tips to help you comply with this requirement when undertaking casework:

- When a constituent makes contact with you, get into the habit of checking that any contact information you hold for them is current, accurate and up-to-date.

- When collecting personal data, take care recording the data and confirm/repeat the information back to the individual to ensure that you have recorded it correctly.

- Where personal data changes, update your records promptly and double check the information that you have entered.

- Watch out for typing errors, especially when entering house and telephone numbers and email addresses!

- If receiving personal data via a third party, take reasonable steps to verify the accuracy of the data where required. Don't assume it's always right!

- Correct incorrect information promptly.

Retention
A Data Controller must not hold personal data for longer than is needed in relation to the purpose for which it was collected. You must also be able to justify the length of time you are keeping personal data for.

If a Member uses an SDDC email account and laptop to conduct casework they are able to request any pertinent data when leaving office. If no such request is made, the Council shall delete emails and files in line with its protocol.

5.0 Communicating with individuals.

This section highlights the main risks associated with sending personal, sensitive or confidential information by email, letter, fax or social media messages. Members should select the most appropriate method of communication taking into consideration the volume and sensitivity of the information being communicated.

5.1 Communication via Email

When undertaking official Council duties, Members must use their Council email account, i.e. <name>@southderbyshire.gov.uk for all communications.

When undertaking casework, it is strongly recommended that Members use their Council email account to communicate with constituents.

Members may send the Council content from their personal addresses in relation to their casework, however personal email addresses cannot be used when undertaking official Council duties and as the data controller they must ensure the appropriate level of security and procedure is in place.

If a Member uses personal email accounts to conduct casework they are the sole data controller and will be responsible for reporting any data incidents to the ICO. If a Member uses their @southderbyshire.gov.uk email account the Council will at that point become an independent data controller with responsibility to keep data collected by the Member safe on the Council's network.

Any use of the Council's email system, whether a Member is using it for official Council duties or for casework use, must be used in line with terms set out in the Member ICT Policy.

Are Council emails secure?

Internal emails:
Emails sent internally within the Council <name>@ southderbyshire.gov.uk email account to another <name>@southderbyshire.gov.uk are secure. This means that the email is unlikely to be intercepted as the email never leaves the Council's network.

Emails to other public bodies:

Emails to and from a <name>@ southderbyshire.gov.uk email account, other Local Authorities and key partner organisations such as Central Government, the LGA, Police Authorities, DWP, are considered secure as the messages are encrypted in transit. This means, if the email is intercepted it's unlikely that the content of the email can be read by others because it is encrypted.

External emails:

Emails sent from a <name>@ southderbyshire.gov.uk email account to an external recipient (e.g. Gmail, Hotmail or private business accounts, etc.) cannot be guaranteed as being secure (as standard), as it depends on the security measures that have been implemented by the email provider of the recipient.

When sending emails where interception could compromise the freedoms of recipients or data subjects an additional level of security can be added to the email via outlook by clicking on the 'Sensitivity' button in a new message and selecting 'Official -Sensitive'. Note, this will change how the email is received and will require the recipient to take an extra step in order to read the message.

Are private / free email accounts secure?
Emails sent to and from private/free email accounts such as Gmail, Hotmail, etc. cannot be guaranteed as secure as it depends on the security measures that have been implemented by the email provider.

Before signing up to a private/free email account it is advisable to check the provider's terms and conditions and read their privacy notice to find out:

- What level of security they offer.
- In which country your emails will be stored.
- Whether they scan the content of your emails and if so why.
- Whether they use your information for any other purpose other than to manage your account.

In addition, before utilising a private/free email account to communicate personal data, Members should consider the following and form a view on the adequacy and appropriateness of using email to facilitate the enquiry:

- The nature of the enquiry.
- The sensitivity of the information.
- The number of individuals the information relates to.
- The potential impact on the individuals should the email be intercepted and the information
- contained within the email becomes known to others etc.

Sending personal information by email?

Email
In addition to the 'technical' risks mentioned above (i.e. email being intercepted whilst in transit) and the risk of a phishing attack, the biggest risks associated with using email for communicating personal, sensitive or confidential information are:

- The email could be sent to the wrong email address.
- Recipients could be copied in by mistake.
- The wrong attachment could be sent with the email.

How can I reduce those risks?

- Double check that you have the right email address.
- Double check that you have typed in the email address correctly. Ensure that you have included all letters, numbers and symbols.
- When selecting the recipient from the Council's global address list or the auto-populate list, ensure that you have selected the right person and be aware of users with the same/similar names.
- Check that you have not 'copied in' anyone by mistake.

Multiple Recipients:

- If using a distribution list, make sure that the members are up-to-date. Remember – local distribution lists are managed by you, not ICT. Updates to corporate distribution lists are made when a service manager or the Leadership Team compile a request for the list to be amended.

- When sending an email to multiple recipients who are not known to each other, use the 'Blind Carbon Copy (BCC)' function to protect the confidentiality of the recipients email addresses.
- When sending personal, sensitive or confidential information to a 'generic' inbox, such as customerservices@southderbyshire.gov.uk, be mindful that the email may be seen by any recipient who has access to that mailbox.

Attachments:

- Be careful when inserting attachments – ensure you have attached the right document(s).
- Once attached to the email, open the attachment and double check it is the right document before you send.

And finally, be careful and take your time when composing the email. Double check everything before you press send. Remember that most emails will be disclosable under Freedom of Information requests so content must be appropriate.

What if I send an email containing personal or confidential information to the wrong person?
Email errors involving personal information are one of the most common causes of personal data breaches. Despite anyone's best efforts, mistakes will happen and when they do it's important that you deal with the error promptly. The following steps should be taken in the event of an email containing personal of confidential information being sent to the wrong person:

1) Immediately recall the message in Outlook.

2) If you can, obtain the contact number of the recipient. Contact them to request that the email be deleted. Ask them to confirm by email that this has been done, and also as then to confirm that the email content has not been forwarded or disclosed to anyone else.

3) Notify the Council's Monitoring Officer and Data Protection Officer of the error.

4) Keep copies of any relevant correspondence to show you have taken all relevant steps to recover the email (this may be needed for any Information Management investigation that may be required).

5.2 Communication via Letter

What are the risks?

- The wrong address and/or recipient could be written on the envelope.
- The wrong information could be included in the envelope.
- The letter could be lost in transit - delivery and receipt of the letter can't be guaranteed in all cases.
- Information could be delivered to wrong address even if the right address is on the envelope.
- Information in paper from is not protected if lost, stolen or seen by
- others.

How can I reduce the risks?

- Double check that you have the correct address
- Ensure the address is correct on the envelope and clearly stated.
- Always include a postcode.
- Always address the letter to a named individual.
- When sending to a company, where possible mark the envelope for the attention of a named individual and their department.
- Ensure the envelope is fit for purpose and can withstand transit. Use tamper proof envelopes where required or seal the information in a double envelope.
- Ensure a return address and contact name is marked on both the outer and inner envelope so that it can be returned to you by the mail service in the event of non-delivery.
- Double check that correct information is enclosed.
- Ensure the information enclosed is also addressed
- Select the most appropriate postal method for the letter based on the sensitivity and volume of the information being sent, e.g. special delivery if you require full tracking and proof of delivery, etc.
- It is good practice to let the receipt know when and how you are sending the information then and to ask them to confirm receipt.

5.3 Communicating via Social Media

Social media is an increasingly popular means of communication that allows people greater freedom and choice in how they communicate both socially and for business purposes. For many it is now the preferred way of finding out what's going on in the local area or contacting a business or organisation.

Using social media when undertaking Council duties will be co-ordinated via the Communication team and Elected Members should not represent the Council using social media in this capacity.

Personal social media accounts and messaging services such as Facebook, Messenger, WhatsApp, etc. must not be used to conduct official Council Business.

Using Social Media for casework
As the Data Controller Members are free to decide whether they wish to use social media as a platform to communicate with constituents when undertaking casework. Should a Member wish to use social media it is recommended that the following guidance is observed:

Open groups/forums/chatrooms:

- Never communicate with constituents on personal matters in a public forum etc.
- Should a constituent contact you via an open forum regarding a personal matter you should advise them to contact you directly via a more appropriate private communication channel (e.g. email, telephone, in person, etc.)

Separating personal from professional
This separation of personal and professional will provide you with greater privacy and may provide you with greater engagement, allowing your local residents to engage with you as a Councillor without the need to become your 'friend'. It also will allow you to undertake casework without using your personal social media account.

You can make use of stringent privacy settings if you do not want your personal social media account to be accessed by the press or public. However, it's important to note that even the strictest privacy settings are no guarantee for posts or actions to remain private.

6.0 Data Breaches

This section outlines what responsibilities a Data Controller has in relation to personal data breaches and what to do in the event of a breach.

What is a personal data breach?
A personal data breach is an incident that affects the confidentiality, integrity and / or availability of personal data.

It is not possible to detail every single incident that may result in a breach, but instances would typically include:

- The theft or loss of personal data or devices that hold such data.

- Inappropriate disclosure of personal data (e.g. an email being sent to the wrong recipient, wrong information in a letter).

- Unlawful access to personal data (e.g. an officer accessing a service user's record with no legitimate business reason for doing so).

- A computer virus that affects Council data.

What does the law require in the event of a personal data breach?
The controller must investigate any breach of personal data and keep a record of that breach.
Where there has been a serious breach, the controller may also be required to inform the Information Commissioner's Office, and in some instances the individual whose personal data has been affected. This must be done within 72 hours of becoming aware the breach.

The data controller must also keep a record of any personal data breach regardless of whether the ICO and/or individual is informed.

Should you encounter a potential, suspected or actual breach of personal data you must report the matter immediately to the Council's Data Protection Officer or any other senior manager in their absence (dataprotectionofficer@southderbyshire.gov.uk) It is recommended that this be done by telephone rather than an email to ensure that the matter is dealt with promptly.

When reporting, you should provide as much information as possible so that the Data Protection Officer can assess the severity of the breach and make an informed decision on whether the matter is to be reported to the ICO and the individual who is affected by the breach. This should include:

- A description of the data breach

- The type and sensitivity of the information affected by the breach.

- Number of individuals affected.

- Whether the breach could put anyone at risk.

- Any action taken to recover/contain the situation.

7.0 Information Rights

Data protection legislation gives rights to individuals. There are several rights including the right to be informed, right of access, right to rectification, right to erasure.

This section focuses on the right of access which is one of the most commonly exercised rights. It explains how a request can be made and how it should be handled.
For details on the other rights please see the ICO's website or contact the Information Management team. Please note that the right to be informed has already been covered in Section 2 of the guide.

What is the right of access?
Individuals have the right to access the personal data that a Controller holds about them. Such a request is commonly referred to as a Subject Access Request (SAR). Individuals are not entitled to the information of anyone else under this right.

A SAR can be made in writing, e.g. mail, letter or through the completion of a SAR form. A SAR can also be made verbally, e.g. in person or over the telephone.
Once a request has been made and the identity of the requestor verified, the Controller has one month to provide the information.

7.1 Who is responsible for responding to a SAR?

It is the responsibility of the Council to respond to any SAR for personal data that is held by the Council. This includes any personal data that may held by a Member for the purpose of undertaking their official Council duties.

What should I do if I receive a SAR from an individual for their personal data?
Should a Member receive a SAR directly from an individual, the request must be forwarded (without delay) to the data protection officer by email (dataprotectionofficer@southderbyshire.gov.uk). Upon receipt of the SAR, the DPO will validate and acknowledge the request to the individual.

Should the scope of the request include information held by a Member (for the purpose of official Council duties), the Data Protection Officer and the Council's Monitoring Officer will work with the Member to identify the requested information and respond to the individual within the relevant timescale.

7.2 Subject Access Requests for personal information relating to casework

It is the responsibility of the Member to respond to any request received from an individual for personal information that is held by a Member in relation to casework.

How should a Member respond to a SAR?

The following suggests the key steps that may be taken by Members when responding to a request. Alternatively, the Member may wish to contact the Council's Data Protection Officer who will support the Member in responding to a SAR:

- Step 1 - Confirm the identity of the requestor, calculate the deadline for response and formally acknowledge the request.
- Step 2 – Locate the information, searching all electronic and paper records held. Collate the information covered by the request.
- Step 3 - Review the information, redacting any information relating to others.
- Step 4 – Decide how you will provide the information to the individual explaining anything that they may not understand (abbreviations, etc.).
- Step 5 – Review and double check the information ready for release.
- Step 6 – Provide the information to the individual. Keep a record of the information provided for any future enquiry.

REPORT TO:	**FINANCE AND MANAGEMENT COMMITTEE**	**AGENDA ITEM: 10**
DATE OF MEETING:	**05 OCTOBER 2023**	**CATEGORY: DELEGATED**
REPORT FROM:	**STRATEGIC DIRECTOR (CORPORATE RESOURCES)**	**OPEN**
MEMBERS' CONTACT POINT:	**DEMOCRATIC SERVICES 01283 59 5722/5889**	**DOC:**
SUBJECT:	**COMMITTEE WORK PROGRAMME**	**REF:**
WARD(S) AFFECTED:	**ALL**	**TERMS OF REFERENCE: G**

1.0 Recommendations

1.1 That the Committee considers and approves the updated work programme.

2.0 Purpose of Report

2.1 The Committee is asked to consider the updated work programme.

3.0 Detail

3.1 Attached at Annexe 'A' is an updated work programme document. The Committee is asked to consider and review the content of this document.

4.0 Financial Implications

4.1 None arising directly from this report.

5.0 Background Papers

5.1 Work Programme.

Annexe A

Finance and Management Committee
Work Programme for the Municipal Year 2023/24

Work Programme Area	Date of Committee Meeting	Contact Officer (Contact details)
Corporate Plan 2020-24: Performance Report (2022-2023 Quarter 4 – (1 April to 31 March)	08 June 2023	Clare Booth Corporate Performance & Policy Officer (01283) 595788
Consultation of Customer Access Strategy 2023-2026	08 June 2023	Catherine Grimley Head of Customer Services (07979149583)
Treasury Management Annual Report	20 July 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Final Revenue Budget Out-turn 22-23	20 July 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Final Capital Out-turn 22-23	20 July 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Corporate Plan 2020-24: Performance Report (2023-2024 Quarter 1 – (1 April to 30 June)	24 August 2023	Clare Booth Corporate Performance & Policy Officer (01283) 595788
Q1 Quarterly Budget Monitoring Report	24 August 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk

Q1 Treasury Management Report	24 August 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Comments, Compliments, Complaints and Freedom of Information Requests 01 October 2022 to 31 March 2023	24 August 2023	Tracy Bingham Strategic Director (Corporate Resources) Tracy.bingham@southderbyshire.gov.uk
Budget Setting Approach 2024/25	05 October 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Long Term Lease of Shardlow Allotments to Shardlow and Great Wilne Parish Council (Exempt)	05 October 2023	Sean McBurney Head of Cultural and Community Services Sean.mcburney@southderbyshire.gov.uk
Write off: Council Tax Business Rates Benefit Overpayment (Exempt)	05 October 2023	Catherine Grimley Head of Customer Services Catherine.grimley@southderbyshire.gov.uk
Sharpe's Pottery Heritage and Arts Trust (Exempt)	05 October 2023	Mike Roylance Head of Economic Development Mike.roylance@southderbyshire.gov.uk
Regrade of Post – Project Officer Environment (HO132) (Exempt)	05 October 2023	Paul Whittingham Head of Housing Paul.whittingham@southderbyshire.gov.uk
Outstanding Internal Audit Recommendations	05 October 2023	Tracy Bingham Strategic Director (Corporate Resources) Tracy.bingham@southderbyshire.gov.uk

Devolution Retrofit Funding	05 October 2023	Craig Lodey Low Carbon Homes Manager Craig.lodey@southderbyshire.gov.uk
IT Protocol	05 October 2023	Anthony Baxter Head of Business Change, Digital & ICT Anthony.baxter@southderbyshire.gov.uk
Q2 Quarterly Budget Monitoring Report	23 November 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Q2 Treasury Management Report	23 November 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Draft Consolidated Budget 2024-25	23 November 2023	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Corporate Plan 2020-24: Performance Report (2023-2024 Quarter 2 – (1 July to 30 September)	23 November 2023	Clare Booth Corporate Performance & Policy Officer (01283) 595788
Environmental Services Commercialisation Plan Review	23 November 2023	Matt Holford (Head of Environmental Services) Matt.holford@southderbyshire.gov.uk
Comments, Compliments, Complaints and Freedom of Information Requests 1 April 2023 to 30 September 2023	23 November 2023	Tracy Bingham Strategic Director (Corporate Resources) Tracy.bingham@southderbyshire.gov.uk

Climate and Environmental Action Plan Review	23 November 2023	Matt Holford (Head of Environmental Services) Matt.holford@southderbyshire.gov.uk
Electric Recharge Infrastructure	23 November 2023	Matt Holford (Head of Environmental Services) Matt.holford@southderbyshire.gov.uk
Draft 2024-25 General Fund Revenue Budget	11 January 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Draft 2024-25 HRA Budget	11 January 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Draft Capital Programmes 2024-25 to 2028-29	11 January 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Treasury Management Strategy & Prudential Indicators	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Capital Strategy	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Final 2024-25 General fund Revenue Budget	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk

Final 2024-25 HRA Budget	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Final Capital Programmes 2024-25 to 2028-29	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Council Tax Setting	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Annual Report of the Section 151 Officer	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Medium Term Financial Strategy	15 February 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Q3 Quarterly Budget Monitoring Report	14 March 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Q3 Treasury Management Report	14 March 2024	Charlotte Jackson Head of Finance Charlotte.jackson@southderbyshire.gov.uk
Proposed Policy for Paying Market Supplements	TBC	Fiona Pittam (Head of Organisational Development & Performance) Fiona.pittam@southderbyshire.gov.uk