Worcestershire County Council

Agenda

Corporate and Communities Overview and Scrutiny Panel

Monday, 23 May 2022, 2.00 pm
County Hall, Worcester

All County Councillors are invited to attend and participate

This document can be provided in alternative formats such as Large Print, an audio recording or Braille; it can also be emailed as a Microsoft Word attachment. Please contact Scrutiny on telephone number 01905 844965 or by emailing scrutiny@worcestershire.gov.uk

Find out more online:
www.worcestershire.gov.uk

worcestershire county council

DISCLOSING INTERESTS

There are now 2 types of interests:
'Disclosable pecuniary interests' and 'other disclosable interests'

WHAT IS A 'DISCLOSABLE PECUNIARY INTEREST' (DPI)?

- Any **employment**, office, trade or vocation carried on for profit or gain
- **Sponsorship** by a 3rd party of your member or election expenses
- Any **contract** for goods, services or works between the Council and you, a firm where you are a partner/director, or company in which you hold shares
- Interests in **land** in Worcestershire (including licence to occupy for a month or longer)
- **Shares** etc (with either a total nominal value above £25,000 or 1% of the total issued share capital) in companies with a place of business or land in Worcestershire.

NB Your DPIs include the interests of your spouse/partner as well as you

WHAT MUST I DO WITH A DPI?

- **Register** it within 28 days and
- **Declare** it where you have a DPI in a matter at a particular meeting
  - you must **not participate** and you **must withdraw**.

NB It is a criminal offence to participate in matters in which you have a DPI

WHAT ABOUT 'OTHER DISCLOSABLE INTERESTS'?

- No need to register them but
- You must **declare** them at a particular meeting where:
  You/your family/person or body with whom you are associated have a **pecuniary interest** in or **close connection** with the matter under discussion.

WHAT ABOUT MEMBERSHIP OF ANOTHER AUTHORITY OR PUBLIC BODY?

You will not normally even need to declare this as an interest. The only exception is where the conflict of interest is so significant it is seen as likely to prejudice your judgement of the public interest.

DO I HAVE TO WITHDRAW IF I HAVE A DISCLOSABLE INTEREST WHICH ISN'T A DPI?

Not normally. You must withdraw only if it:

- affects your **pecuniary interests OR**
  relates to a **planning or regulatory** matter
- **AND** it is seen as likely to **prejudice your judgement** of the public interest.

DON'T FORGET

- If you have a disclosable interest at a meeting you must **disclose both its existence and nature** – 'as noted/recorded' is insufficient
- **Declarations must relate to specific business** on the agenda
  - General scattergun declarations are not needed and achieve little
- Breaches of most of the **DPI provisions** are now **criminal offences** which may be referred to the police which can on conviction by a court lead to fines up to £5,000 and disqualification up to 5 years
- Formal **dispensation** in respect of interests can be sought in appropriate cases.

Simon Mallinson Head of Legal and Democratic Services July 2012 WCC/SPM summary/f

worcestershire
countycouncil

Corporate and Communities Overview and Scrutiny Panel
Monday, 23 May 2022, 2.00 pm, Council Chamber

Membership

Councillors:

Cllr Mike Rouse (Chairman), Cllr James Stanley (Vice Chairman), Cllr Mel Allcott, Cllr Aled Evans, Cllr Laura Gretton, Cllr Peter Griffiths, Cllr Emma Marshall, Cllr Natalie McVey and Cllr Craig Warhurst

Agenda

Item No	Subject	Page No
1	**Apologies and Welcome**	
2	**Declarations of Interest and of any Party Whip**	
3	**Public Participation** *Members of the public wishing to take part should notify the Assistant Director for Legal and Governance in writing or by e-mail indicating both the nature and content of their proposed participation no later than 9.00am on the working day before the meeting (in this case Friday 20 May). Further details are available on the Council's website. Enquiries can also be made through the telephone number/e-mail address listed in this agenda and on the website.*	
4	**Confirmation of the Minutes of the Previous Meeting** Previously circulated	
5	**Refresh of the Scrutiny Work Programme 2022/23** (Indicative timing 2:05 – 2:20pm)	1 - 6
6	**The Council's Policy on Support for Refugees** (Indicative timing 2:20 – 3:00pm)	7 - 16
7	**Council Compliance with Freedom of Information and Data Protection Legislation** (Indicative timing 3:00 – 3:40pm)	17 - 24
8	**The Council's Implementation of Microsoft Intune (Mobile Device Management)** (Indicative timing 3:40 – 4:15pm)	25 - 38

Agenda produced and published by the Assistant Director for Legal and Governance, County Hall, Spetchley Road, Worcester WR5 2NP. To obtain further information or hard copies of this agenda, please contact Emma James/Jo Weston 01905 844965, email:scrutiny@worcestershire.gov.uk

All the above reports and supporting information can be accessed via the Council's Website

Date of Issue: Friday, 13 May 2022

This page is intentionally left blank

worcestershire
countycouncil

CORPORATE AND COMMUNITIES OVERVIEW AND SCRUTINY PANEL 23 MAY 2022

REFRESH OF THE SCRUTINY WORK PROGRAMME 2022/23

Summary

1. The Communities Overview and Scrutiny Panel (the Panel) is being asked to consider suggestions for its 2022/23 Work Programme prior to it being submitted to Council for approval.

Background

2. The Panel routinely reviews its work programme at each meeting to consider which issues should be investigated as a priority.

3. In addition, on an annual basis, the rolling annual Work Programme for Overview and Scrutiny is approved by Council. The current Work Programme was agreed by OSPB on 21 July and was approved by Council on 9 September 2021.

Scrutiny Work Programme 2022/23

4. The Scrutiny Work Programme for 2022/23 is now being refreshed. Panel Members and other stakeholders have been invited to suggest topics for future scrutiny.

5. The suggestions are detailed on the draft Work Programme (attached at Appendix 1).

6. Members are asked to consider the draft Work Programme and agree its priorities for 2022/23. Issues should be prioritised by using the scrutiny feasibility criteria agreed by OSPB.

Feasibility Criteria

7. The criteria (listed below) will help to determine the scrutiny programme. A topic does not need to meet all of these criteria to be scrutinised, but they are intended as a guide for prioritisation.

- Is the issue a priority area for the Council?
- Is it a key issue for local people?
- Will it be practicable to implement the outcomes of the scrutiny?
- Are improvements for local people likely?
- Does it examine a poor performing service?
- Will it result in improvements to the way the Council operates?
- Is it related to new Government guidance or legislation?

8. The Overview and Scrutiny Performance Board will receive feedback on the Scrutiny Panels' discussions and agree the final scrutiny work programme at its 25 May meeting. Council will be asked to agree the Work Programme at its meeting on 14 July.

Remit of the Panel

9. The Corporate and Communities Overview and Scrutiny Panel is responsible for scrutiny of:

- Commissioning, contracts and commerce and ensuring the corporate commissioning cycle works well
- Transformation
- Finance
- Localism and Communities
- Organisation and employees

10. The current Work Programme was discussed by the Overview and Scrutiny Performance Board (OSPB) on 21 July 2021 and agreed by Council on 9 September 2021.

Dates of Future 2022 Meetings

- 6 July at 2pm
- 21 September at 10am
- 14 November at 2pm

Purpose of the Meeting

11. The Panel is asked to consider and prioritise the draft 2022/23 Work Programme and consider whether it would wish to make any amendments. The Panel will wish to retain the flexibility to take into account any urgent issues which may arise.

Supporting Information

Appendix 1 – Corporate and Communities Overview and Scrutiny Panel Draft Work Programme 2022/23

Contact Points

Emma James / Jo Weston, Overview and Scrutiny Officers, Tel: 01905 844964 / 844965
Email: scrutiny@worcestershire.gov.uk

Background Papers

In the opinion of the proper officer (in this case the Assistant Director for Legal and Governance), the following are the background papers relating to the subject matter of this report:

- Agenda and minutes of OSPB on 21 July 2021
- Agenda and minutes of Council on 9 September 2021

This page is intentionally left blank

Corporate and Communities Overview and Scrutiny Panel

Date of Meeting	Issue for Scrutiny	Date of Last Report	Notes/Follow-up Action
23 May 2022	The Council's Policy on all Refugees		Panel Member suggestion March 2022
	Council Compliance with Freedom of Information and Data Protection Legislation		Agenda planning October 2021
	The Council's Implementation of Microsoft Intune (Mobile Device Management)		Panel request April 2022
6 July 2022	Performance and In-Year Budget Monitoring (Q4 Outturn January 2022 – March 2022)	17 March 2022 8 November 2021 20 July 2021	
	Update on the Libraries Strategy/transformation (post Covid-19) – to include the E-Library		Panel Member suggestion July and September 2021
	Liquidlogic		Panel member suggestion February 2022
21 September 2022	Performance and In-Year Budget Monitoring (Q1 April – June 2022)		
	Performance monitoring of comments, compliments and complaints	8 November 2021 20 July 2021 11 March 2021	
	Gypsy/Traveller Services		Panel member suggestion March 2022
	Community Engagement (Here2Help)	24 September 2021	
14 November 2022	Performance and In-Year Budget Monitoring (Q2 July – September 2022)		
	Update on the Procurement Strategy		
	Update on the Councils Strategy for Museums, Arts and Culture		
Possible Future Items			
TBC	Performance monitoring of comments, compliments and complaints	8 November 2021 20 July 2021	

		11 March 2021	
TBC	West Mercia Energy Joint Committee Business Plan	17 January 2022	
TBC	Data Analytics - Power BI Strategy - Instant Atlas - Framework for publicly accessible data	17 January 2022	
TBC	How the Council Supports Volunteers and Volunteering		Chairman suggestion April 2022
TBC	Worcestershire One Public Estate		Agreed by Panel 14 February 2022
TBC	Electric Vehicle charging points on the County Council Estate		Agreed by Panel 14 February 2022
TBC	Performance of registration of deaths within 5 days	8 November 2021	Agreed by Panel 8 November 2021
TBC	Council Communication	8 November 2021	Agreed by Panel 8 November 2021
Standing Items			
November/January	Budget Scrutiny		
	Annual update on the Council's energy purchasing arrangement via the West Mercia Energy Joint Committee including the Business Plan	17 January 2022	Agreed at October 2021 Overview and Scrutiny Performance Board
TBC	Councillors Divisional Funding Scheme	20 July 2021	
TBC	Worcestershire County Council Regulation of Investigatory Powers Act 2000 Policy (RIPA)		

worcestershire
countycouncil

CORPORATE AND COMMUNITIES OVERVIEW AND SCRUTINY PANEL 23 MAY 2022

THE COUNCIL'S POLICY ON SUPPORT FOR REFUGEES

Summary

1. The Corporate and Communities Overview and Scrutiny Panel has requested an overview of the Council's policy on support for Refugees.

2. The Cabinet Member with Responsibility for Communities and the Assistant Director for Communities have been invited to attend the meeting to respond to any questions from Panel members.

Background

3. The war in Ukraine and the plight of Ukrainian people seeking refuge in other countries has prompted Central Government to introduce schemes of support. Worcestershire's response to the situation in Ukraine has been discussed at recent meetings of the Overview and Scrutiny Performance Board on 23 March/26 April and Cabinet on 24 March (see background papers), and this has prompted this Panel to seek an overview of the Council's overall policy on support for refugees.

The Resettlement Programmes

4. Worcestershire are currently involved in four resettlement programmes:

   a. UK Resettlement Scheme (UKRS) previously Vulnerable Persons Resettlement Scheme (VPRS)
   b. Afghan Relocation Assistance Policy
   c. Afghan Citizen Refugee Scheme
   d. Homes for Ukraine Scheme

UK Resettlement Scheme (UKRS)

5. **The Vulnerable Persons Resettlement Scheme** (VPRS) was launched by the UK government in 2014 to resettle the most vulnerable refugees affected by the Syrian crisis. In 2015, in response to the growing Syrian refugee crisis, the UK pledged to resettle 20,000 refugees fleeing the Syrian conflict by March 2020. These 20,000 refugees would be part of the Vulnerable Persons Resettlement Scheme (VPRS).

6. This scheme changed in April 2021 and became the **UK Resettlement Scheme**

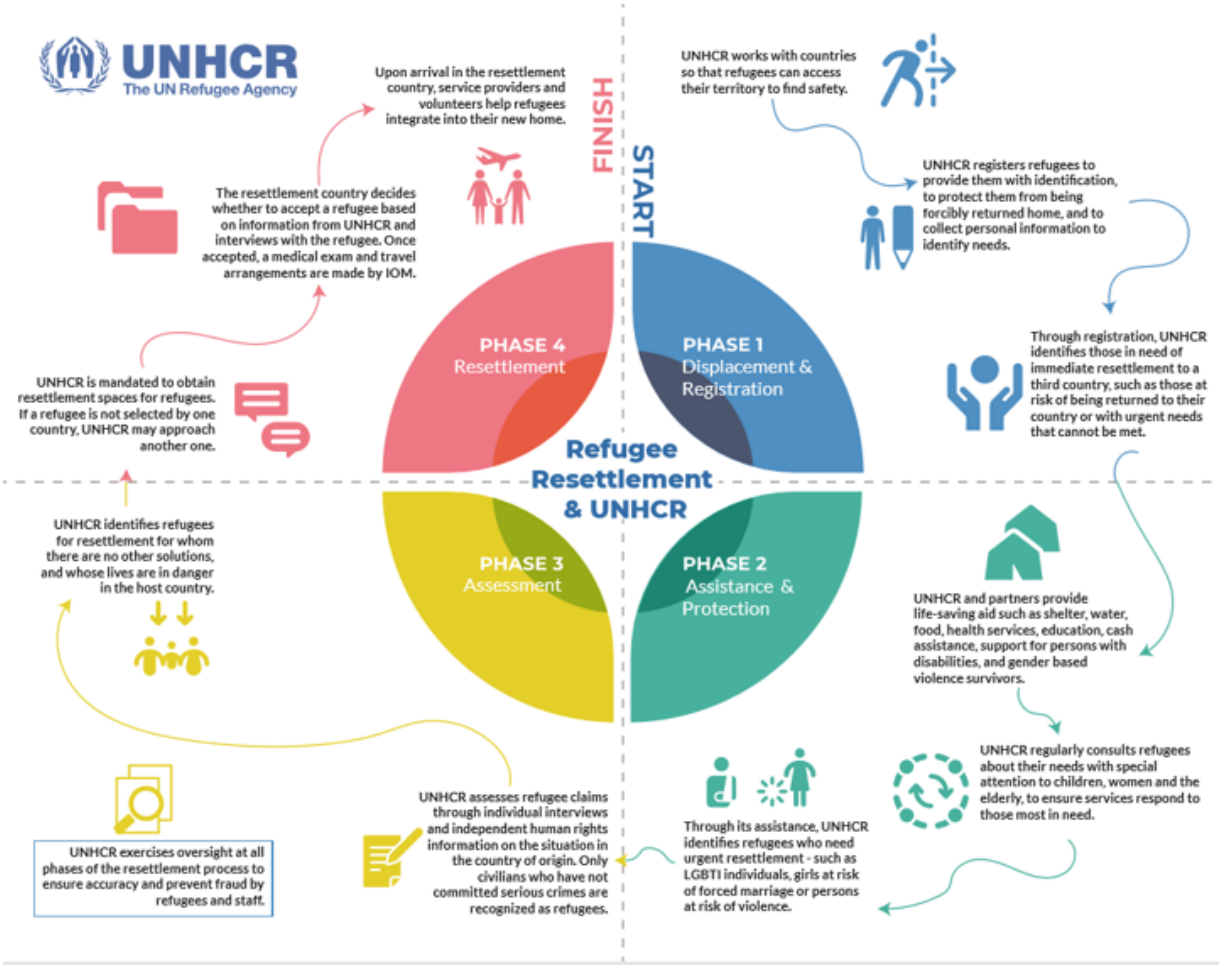
(UKRS) which extended the programme to refugees across the globe, although currently the focus remains on Syrian refugees.

7. The UK Government relies on United Nations High Commissioner for Refugees (UNHCR) to help them identify and process vulnerable refugees who would benefit from resettlement. UNHCR has responsibility for all out-of-country casework activity relating to UKRS, and will:

- verify identity and family composition.
- interview registered refugees to determine their experiences and current circumstances in the host country.
- identify refugees with potential resettlement needs and assess their vulnerability.
- conduct a full Refugee Status Determination (RSD); and
- conduct a resettlement interview and assess that refugees meet the criteria for resettlement before referring them to the UK for consideration.

8. UNHCR will conduct interviews with the family as they are mandated to determine whether an individual meets the 1951 Convention definition of a refugee and are best placed to assess their protection needs. Having determined that the individual is a refugee, UNHCR will then consider whether resettlement is the right long-term solution for them, and then to which country or resettlement scheme they should be referred. Refugees do not decide which country they are referred to, rather UNHCR looks at available quotas and decides which country criteria the family best fits.

9. Refugees are assessed for resettlement by UNHCR against their resettlement submission categories shown in the graph below:



10. Worcestershire became involved with the Vulnerable Persons Resettlement Programme 7 years ago. Since then, 102 people have been resettled in the first two cohorts. Worcestershire's Local Authority Leaders agreed to a further 50 individuals as part of cohort 3 which began arriving in November 2021.

11. The Government is continuing to review the programme in light of further programmes that have come online, especially in terms of funding. Worcestershire receives funding from central government on a sliding scale over the five years the refugee forms part of the programme. The current commitment has been agreed with the current funding level, which is: -

- Year One - £8,500 per person
  - £2,250 per child ages 3 and 4
  - £4,500 per child aged 5 to 18
  - £850 per adult (over 19) for ESOL (English Language support)
- Year Two - £5,000 per person
- Year Three - £3,700 per person
- Year Four - £2,300 per person
- Year Five - £1,000 per person

12. It is expected that over the course of the programme, that any extended needs are absorbed into the normal council budgets as for any resident of Worcestershire.

Afghan Relocation Assistance Policy

13. The Afghan Relocation Assistance Policy (ARAP) was launched to support the relocation of current and former locally employed staff by HM Government who were assessed to be at serious risk. Announced in January 2021, this programme has been open since April 2021 and the Councils of Worcestershire agreed to welcome 30 people to our County.

Afghan Citizen Refugee Scheme

14. The Government have also announced that there will be a further programme, the Afghan Citizen Refugee Programme (ACRS) and the Government aims to resettle c20,000 people over five years under this new scheme. This will include the recently evacuated and those referred by UNCHR from Afghanistan or other third countries. The scheme will prioritise those who have assisted the UK efforts in Afghanistan and stood up for values such as democracy, women's rights, freedom of speech, and rule of law and vulnerable people, including women and girls at risk, and members of minority groups at risk (including ethnic and religious minorities and LGBT+).

15. The Councils of Worcestershire have agreed to welcome 200 people over 5 years. The first arrivals under this scheme came in September 2021.

16. In the Autumn of 2021 the Government requested that the pledges made by Local Authorities for the two Afghan programmes were merged in order that the number of arrivals under the ARAP scheme could be accommodated. This is because many Afghans and their families are still being hosted in bridging hotels.

17. On that basis, Worcestershire's resettlement to date has been 66 in total (since September 2021).

18. The two Afghan programmes are 3 years in duration and funding is as follows.

- Year One - £10,500 per person
    - £2,250 per child ages 3 and 4
    - £4,500 per child aged 5 to 18
    - £850 per adult (over 19) for ESOL
- Year Two - £6,000 per person
- Year Three - £4,020 per person

Homes for Ukraine

19. This scheme, launched on 14 March 2022, is open to Ukrainian nationals who were residents in Ukraine prior to 1 January 2022 and their immediate family who may be of other nationalities, to be sponsored to come to the UK. Applicants can apply from Ukraine or from any other third country. The scheme allows individuals to sponsor named Ukrainians.

20. Children under the age of 18 must be applying as part of a family unit which includes their parent or legal guardian to be eligible for the scheme. That family unit must stay together in the same sponsor accommodation. Children who are currently outside of the UK can use the scheme to reunite with their parent or legal guardian who is currently living in the UK, if they are the child's sponsor. Unaccompanied

children who are under 18 are not allowed to be sponsored by, or reside with, unrelated sponsors, unless they are their legal guardian.

21. Around 150,000 individuals across the UK have registered interest in being a sponsor, c2400 in Worcestershire. People arriving under this scheme will be able to:
    - Live and work in the UK for up to three years
    - Access healthcare, benefits, employment support, education, and English language tuition

22. Most will be women and children and older people, as able-bodied men aged 18 to 60 are not generally being allowed to leave Ukraine at present. More detailed information on the expectation of sponsor households can be found here. Homes for Ukraine scheme: frequently asked questions - GOV.UK (www.gov.uk).

23. This scheme does attract additional funding. A £350 per month 'thank you payment' has been offered to sponsors for between 6-12months (6-month period is the minimum expectation set for sponsors). The 'thank you' payment is limited to one payment per residential address and will remain tax free. Payments are expected to be issued once accommodation and DBS checks are carried out.

24. £10,500 per person will also be provided to Local Authorities accepted under this scheme. The funding is "to provide much wider support to families to rebuild their lives and fully integrate into communities" and is paid to Upper Tier authorities on a quarterly basis, in arrears. Worcestershire Local Authorities have agreed to treat this resource as a pool and distribute across the seven authorities.

25. The Government is also providing additional funding to councils to provide education services for children from families arriving from Ukraine under the scheme. The Department for Education (DfE) will allocate funding on a per pupil basis for the three phases of education at the following annual rates:
    - Early years (ages 2 to 4) - £3,000
    - Primary (ages 5 -11) - £6,580
    - Secondary (ages 11-18) - £8,755

26. Councils have several important functions in supporting the Homes for Ukraine scheme. Councils are expected to offer support including accommodation checks, DBS checks on sponsors and other eligible individuals, checks on sponsors, interim payments for guests and thank you payments to sponsors.

27. The Leaders of the councils of Worcestershire agreed that this scheme would be a 'One Worcestershire' approach with the seven local authorities working together. The County Council is utilising its community services to support the programme including Libraries, Here 2 Help, Adult Learning and the Resettlement Team bringing skills and knowledge together to assist with this scheme.

28. The number of people who can access this scheme is uncapped and is dependent on the capacity of the sponsors who come forward. As of the 10 May 2022, the latest information on households and Ukraine guests in Worcestershire is below.

District	No of Host Properties	No of Guests	No of Pre-school age children	No of Primary school age children	No of Secondary school age children
To be confirmed		3	1		
Bromsgrove	38	95	6	14	11
Malvern Hills	83	216	16	45	26
Redditch	18	38	3	8	1
Worcester City	62	130	3	22	23
Wychavon	107	251	14	34	38
Wyre Forest	33	80	7	12	9
Total	**341**	**813**	**50**	**135**	**108**

29. The Homes for Ukraine scheme is different to the **Family Visa Scheme**, which the Local Authority does not participate in. The **Family Visa Scheme** is entirely dependent on whether Ukrainians living in the UK have relatives who want to support those leaving Ukraine. It is estimated there are around 130 Ukrainians in total living in the county according to provisional 2021 census data. This scheme does not attract additional funding, but it is envisaged that Councils will be expected to perform their duties in relation to housing / education etc.

Worcestershire's Resettlement Team

30. Worcestershire County Council has developed a Resettlement Team to lead on the support the individuals and families settling in Worcestershire under the UKRS, ARAP and ACRS schemes. The Team provide support in the following way:

- Co-ordination of appropriate housing and support including: understanding tenancy agreements, utilities, and bills; plus, budgeting skills.
- Cultural awareness and understanding the UK Laws.
- Orientation of area, including accessibility for public transport, religious buildings, and culturally sensitive shops.
- Assisting with access to benefits, employment, training, and education (including ESOL) and higher education for students at post 18.
- Supporting accessibility to all health provisions, including GPs, dentists, opticians, mental health support and specialist services; and
- Providing parents with support for ensuring all children are enrolled in school and helping them understand the processes within a school environment.

31. The team also has an ESOL (English to speakers of other languages) tutor who has continued to provide not only English language lessons, but also creates individual pathways to include well-being, aspirations and goals, employment planning and preparation.

32. There are also several activities and short courses in a variety of subjects to promote independence and building relationships with other refugees. The Team assists in applications for employment, interviews, and transport. In short, the Team help them with every element of their new lives in Worcestershire with the aim of promoting independence as quickly as possible.

33. The aim of the Team is to have families largely independent of the schemes by the end of year 3 (subject to any ongoing needs). For the UKRS scheme the remaining 2 years provide the safety net for those that are independent and with those that require further intervention and transitioning to other support services.

Impact for Worcestershire

34. Worcestershire prides itself on being a welcoming county as demonstrated by its commitment to welcome people to the county through the various schemes. One of the strengths of Worcestershire's communities is the desire to help and assist. The Welcomes Groups, other voluntary sectors, sponsors, and colleagues have all collectively ensured that refugees have been settled into the county.

35. It is fair to say that the various schemes have not come without their challenges. This includes timeliness of notification and guidance from the Government which has prevented plans being pro-actively developed in preparing for arrivals.

36. Access to health, education, and suitable, sustainable housing for those resettling in the County is also becoming increasingly challenging. The level of housing benefit has not kept pace with increased rental costs and therefore finding appropriate housing has become difficult. It is also well-documented the pressures on the health service in terms of GP and dental access as well as access to mental health services. This is only likely to be compounded with additional people arriving in the county through these schemes as well as the general population increase.

Feedback received

37. Whilst it is too early to provide meaningful feedback on the Homes for Ukraine Scheme, the other resettlement schemes have now been in place for some months. A change in operational delivery, implemented in 2020, provided the Resettlement Team with an opportunity to provide a bespoke programme for each person arriving in the county. This change in delivery covered all areas detailed previously, so the team could provide a complete wraparound package of support.

38. The success of introducing this model of working is illustrated in some of the stories below: -

"Sam"

39. Sam fled Syria with nothing when he was 19 years old, arriving in the UK when he was 26. Sam is a well-educated and hard-working individual, having started University before he had to flee. Since arriving here in Worcestershire he has continued to work tirelessly to pass all his English, Maths, and IT Courses at the local college in Bromsgrove. When the Resettlement Team met Sam in December 2019, he told the team of his aspirations, and then the Team worked with him to assist him in fulfilling his dream. Throughout lockdown 1 he studied a variety of online Cabin Crew courses and in September 2020 he successfully gained a place on a Cabin Crew course in Birmingham, which he passed with distinctions this summer and was offered a place on the Ryanair training programme. He is currently working in a local supermarket and has also recently passed his driving theory, whilst he waits for his training at Ryanair to commence. (2) Home Office - Posts | Facebook

“Mazen”

40. Mazen was a very successful journalist prior to arriving in the UK and is a well educated and self-driven individual with the aspiration to “help others”. When the resettlement team first met him, it was clear his direction would be driven by his desire for giving back. The Team have worked to support Maz on his journey to becoming self-employed and he now has an established business in the broadcast industry. His bio for his business is At Maz Broadcast, which focuses on inspiring stories, creating video content to raise awareness in society on a variety of topics. His work to date includes mental health and well-being, adult learning, and a variety of short films about aspect of the local community. You can find him on all social media channels and his website link is below. Maz Broadcast | Creating Inspiring Stories Through Video

41. In lockdown 1, Maz worked tirelessly to support the local covid support group, cycling for miles to deliver prescriptions and this was rewarded by being nominated and winning the Making a Difference, BBC Hereford & Worcester Radio Award which resulted in a train being named after him! Below is a photo of the train being unveiled:

“Amani & Mahmoud”

42. Amani & Mahmoud arrived in Worcestershire in 2016, with their 3 children. Amani was a teacher in her home country, and also worked for the Red Cross whilst in Lebanon focusing on ensuring all children had access to education. Mahmoud was a highly skilled tiler which is a vital trade in Syria. When the resettlement team met this family it was clear they all have the vision to work hard and start a new life in the UK. Both studied constantly to ensure they both passed all the English and IT courses. Mahmoud studied additional training courses in building and forklift driving and now holds a steady job in that field. Amani became a translator for a national organisation, whilst also doing a Teaching Assistant qualification. On completion of the course, Amani began working at a Girls College in Malvern, teaching Arabic and joined the team as the Key Support Worker for the UKRS families for Cohort 2 and beyond. They were the first two people to pass their driving theory and practical and both now have successful jobs within their community.

“Ahmad”

43. Ahmad and his family arrived at the end of 2016. His thirst for learning and

helping others is evident in all he does. His wife also studies hard, completing both Maths and English throughout lockdown, whilst home-schooling the girls. Ahmad has regularly attended college in Birmingham and has passed many English levels and won awards for his efforts. He now works a steady job in the Care Industry and has excelled over the past 3 years. He is a well-loved member of staff at the Care Home, and he has used his love of music to help the residents too, earlier this year he was featured in a video showcasing his work on the Alzheimer's Society Facebook page. Music and Singing | Alzheimer's Society (alzheimers.org.uk)

"Salim"

44. Salim arrived in the county in September 2021 into the bridging hotel along with his wife. They relocated to Worcester City into private permanent accommodation in October. He applied and was successful in obtaining a position within the Resettlement Team whilst continuing to study at college. The Team have supported him through the programme to attend college to improve his IT skills and he is currently learning to drive after passing his theory in January. He is a valuable member of the team.

Purpose of the Meeting

45. The Corporate and Communities Overview and Scrutiny Panel is asked to:
    - consider the information provided in the report
    - determine whether any further information or Scrutiny is required at this stage; and
    - agree any comments to highlight to the Cabinet Member with Responsibility for Communities.

Contact Points

Emma James / Jo Weston, Overview and Scrutiny Officers
Tel: 01905 844965 / 844964, Email: scrutiny@worcestershire.gov.uk

Background Papers

In the opinion of the proper officer (in this case the Assistant Director for Legal and Governance) there are no background papers relating to the subject matter of this report.

- Agenda and Minutes of the Overview and Scrutiny Performance Board on 23 March 2022
- Agenda and Minutes of Cabinet on 24 March 20222

All agendas and minutes are available on the Council's website here

This page is intentionally left blank

worcestershire countycouncil

CORPORATE AND COMMUNITIES OVERVIEW AND SCRUTINY PANEL 23 MAY 2022

COUNCIL COMPLIANCE WITH FREEDOM OF INFORMATION AND DATA PROTECTION LEGISLATION

Summary

1. The Cabinet Member with Responsibility for Corporate Services and Communication (CMR) and the Strategic Director of Commercial and Change have been invited to the meeting to update the Panel on how the Council complies with requests for information made under both freedom of information and data protection legislation.

Background

2. Under the Freedom of Information Act (FOI), people can make a request for any information held by the Council; the Environmental Information Regulations (EIR) provides a broadly similar access route for environmental information.

3. Under data protection legislation (DP), primarily the General Data Protection Regulation and the Data Protection Act 2018, individuals have rights in relation to the information the Council holds about them. This includes the right to be provided with a copy of the information the Council holds about them (a 'subject access request').

4. While the Council must process and consider each request received, the Council does not always have to provide the requester with the information held as exemptions and exceptions may be applied. For example, personal data (information about individuals) would not usually be included in a response to a FOI request which puts the information into the public domain.

UK General Data Protection Regulation and Data Protection Act 2018

5. Following the UK's exit from the European Union (EU), the EU General Data Protection Regulation (EU GDPR) was retained in UK law as the UK GDPR.

6. The Data Protection Act 2018 (DPA 2018) sits alongside and supplements the UK GDPR, for example by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's functions and powers.

7. Under data protection legislation (DP), primarily the UK GDPR and the Data Protection Act 2018, individuals have rights in relation to the information the Council holds about them. This includes the right to be provided with a copy of the information the Council holds about them (a 'subject access request').

8. Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime:

a. Lawfulness, fairness and transparency
b. Purpose limitation
c. Data minimisation
d. Accuracy
e. Storage limitation
f. Integrity and confidentiality (security)
g. Accountability

9. On 28 June 2021, the EU approved adequacy[1] decisions for the GDPR and the Law Enforcement Directive (LED). This means data can continue to flow as it did before, in the majority of circumstances. Both decisions are expected to last until 27 June 2025.

Freedom of Information/Environmental Information

10. Under the Freedom of Information Act (FOI), people can make a request for any information held by the Council; the Environmental Information Regulations (EIR) provides a broadly similar access route for environmental information.

11. Requests can be made to any Council officer, and they do not need to mention the legislation, they do need to ask for 'recorded information' and the requester needs to provide a name. FOI requests need to be put in writing, EIR requests can be made verbally.

12. Both types of requests must be answered within 20 working days commencing the day after the request is received.

13. In FOI, fees can be charged for any hours it will take to respond to a request over the 'appropriate limit' rather than refuse the request (requests can be refused if they will take more than 18 hours to find, extract, and collate the relevant information). However, the first 18 hours cannot be charged for, and the fees notice must be issued before the work is completed.

14. Requests are coordinated by the Corporate Information Governance Team (CIGT), which is part of IT and Digital. They are centrally logged, assessed and allocated to the relevant Directorate or service area Information Access Coordinator (IAC) with any relevant advice about to identify, collate, and respond to the requester.

15. An in-house built request management system, Veritas, is used to manage all FOI and EIR requests and people can make a request directly into the system from the Council's website. The system then manages the whole request process from beginning to end, tracking who has been asked to find information, facilitating the supply of the information to the relevant Information Access Coordinator so the appropriate response can be drafted, to the final response to the request and any disclosure of information requested. The system includes a series of template letters to assist consistent and compliant responses across the whole Council and includes

[1] 'Adequacy' is a term the EU uses to describe countries, territories, sectors or organisations it deems to have an "essentially equivalent" level of data protection to the EU.

facilities to record requests for internal review of our responses and any subsequent referral to the Information Commissioner's Office (ICO).

16. Appendix 1 provides further detail about requests for information under FOI and EIR, including numbers, response times and the service areas they relate to.

Subject Access Requests

17. Under data protection legislation, individuals are entitled to ask the Council for a copy of the personal data it holds about them. This is known as a Subject Access Request (SAR).

18. Requests can be made to any Council officer, and they do not need to mention the legislation and can be made in writing or verbally. The Council will verify the identity of the requester, usually by requesting two documents confirming name, address and date of birth. Requests can be made by third parties (e.g. solicitors) if sufficient authorisation is provided. Requests are subject to a timescale of 1 month, commencing the day the request is received, unless it is considered complex or numerous when a further 2-month extension to be timescale can be applied. A fee cannot be charged for SAR requests unless it is assessed as 'manifestly unreasonable' and the Council decides to process the request rather than refuse the request, or if a request asks for additional copies of information.

19. Requests are centrally coordinated and logged by the Corporate Information Governance Team (CIGT) who provide advice, guidance, and request specific training to officers who are assigned subject access requests to respond to. In respect of requests for information from education and social services (comprising the majority of requests received), a dedicated team in CIGT completes the end-to-end process for Children's Services and Worcestershire Children's First, and the Business Operations Team complete the same for Adult requests.

20. Relevant information is searched for, extracted and then worked through to ensure that any personal data the requester is entitled to receive is identified for disclosure and any information that is subject to an exemption is removed (for example information about other third-party individuals). This is then reviewed by the relevant business area to quality check the disclosure before the information is sent to the requester, usually by Royal Mail Special Delivery.

21. The Council have received the following numbers of subject access requests. As the Council must validate the identity of the requester before a SAR can be processed, some requests do not progress from an enquiry:

Year	SAR enquiries received	Enquiries progressed to full requests	Total cases completed on time	Percentage completed on time
2018/19	221	140	144	65.2%
2019/20	227	128	134	59.0%
2020/21	217	130	143	68.4%
2021/22	237	140	167	72.9%

22. The numbers of enquiries received, their complexity, and their scope are increasing year on year and while this trend was already noticeable, the impact of the General Data Protection Regulation which came into force on 25 May 2018 accelerated this trend. Requests can be extremely time consuming as they need to be carefully processed to ensure that all relevant information is identified, any redactions and exemptions are appropriately applied and checked by the relevant social work contact. Similar to the FOI requests, it is very difficult to calculate the actual time taken to complete each request. For these reasons, it is increasingly difficult to complete requests within the statutory timescale with the current allocated resources and processes.

23. CIGT are working with colleagues in IT to develop a system to more effectively manage SAR and other information sharing requests (for example requests to share data with other organisations), which will enable the requests to be processed more efficiently and keep track of progress.

Information Commissioner Office (ICO) Complaints

24. The ICO has a general duty to investigate complaints from members of the public who believe that an authority has failed to respond correctly to a request for information. If someone makes a complaint against the Council, the ICO complaints handling process gives the Council the opportunity to reconsider its actions and put right any mistakes. Due to the opportunity to resolve complaints informally, in many circumstances there is no formal outcome from the ICO.

25. The ICO can take enforcement action if they consider the complaint has not been resolved informally. For FOI/EIR complaints this is usually a decision notice stating what needs to be put right, but can also include an enforcement notice, information notice, or undertaking. For data protection complaints or concerns this could be an audit, enforcement notice, monetary penalty, or prosecution.

Metric	2021/22
Number of complaints received - Info Commissioner (FOI and EIR)	1
Number of complaints received - Info Commissioner (DP)	6

26. The FOI complaint received during 2021/22 led to a formal decision notice not upholding the complaint made by the requester.

Training and Awareness

27. Information Governance training continues to feature as a key part of ensuring staff are aware of their responsibilities.

28. All staff are required to complete mandatory training modules on FOI/EIR and on DP. These modules are required to be completed every two years, so staff knowledge and awareness remains current. While the main route for completing this training is through eLearning, the training is made available in other formats to meet staff needs and requirements.

29. A more in-depth FOI module has also been launched to support the Directorate Information Access Coordinators who are an integral part of discharging and responding to FOI/EIR requests.

30. Information Governance messages continue to be provided to staff alerting them to the need to protect personal data and use it appropriately. These have included a blog from the Assistant Director for IT and Digital, OurSpace news stories, and updates to the guidance on the Intranet.

Information Asset Register

31. The Council has an Information Asset Register which acts as a mechanism for understanding and managing the Council's information assets and the risks to them.

32. This formed an integral part of the project to implement the changes UK GDPR brought in 2018 and now details the information the Council holds across the authority. It is a living document and is subject to regular review including when there are changes in service provision and delivery for example in-sourcing or out-sourcing of services.

Privacy Notices

33. Privacy Notices are in place and accessible on the Council's website (www.worcestershire.gov.uk/privacy) providing information about the processing of personal data across Council services.

Data Protection Impact Assessment (DPIA)

34. A DPIA is undertaken for processing that is likely to result in a high risk to individuals. It is a process designed to systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of our accountability obligations under the UK GDPR, and when done properly helps assess and demonstrate compliance with data protection obligations.

35. DPIA screenings are used to determine when to do a DPIA, (adhering to ICO guidance 'When do we need to do a DPIA?'). The screenings check whether the processing is on the list of types of processing that automatically require a DPIA, as well as considering other factors that may indicate it is a type of processing that is likely to result in high risk, such as processing the data of vulnerable individuals.

36. A streamlined approach has been taken to assist staff to complete DPIAs to ensure that data protection is built into the design of processes, systems and improvements. As the DPIA is only one of several impact assessments that need to be completed, a cross-discipline group, formed under the CIGB, worked with IT to develop the Joint Impact Assessment (JIA) system that enables staff to complete the

screenings and assessments to identify any impact on data protection, equality, health and environmental sustainability in one place. This ensures consistency of completion, reduces the time taken by officers to complete the assessments, and minimises confusion from multiple processes to follow for separate assessments.

Purpose of the Meeting

37. The Panel is asked to consider the information provided and:
    - determine any comments to make to the Cabinet Member with Responsibility for Corporate Services and Communication
    - agree whether any further Scrutiny is required at this stage.

Supporting Information

Appendix 1 – Requests for information under FOI and EIR

Contact Points

Andrew Spice, Strategic Director of Commercial and Change
Telephone: 01905 846678
Email: aspice@worcestershire.gov.uk

Sandra Taylor, Assistant Director for IT and Digital
Telephone: 01905 845447
Email: staylor12@worcestershire.gov.uk

Emma James / Jo Weston, Overview and Scrutiny Officers
Telephone: 01905 844964
Email: scrutiny@worcestershire.gov.uk

Background Papers

In the opinion of the proper officer, in this case the Assistant Director for Legal and Governance there are no background papers relating to the subject matter of this report:

All agendas and minutes are available on the Council's website here.

worcestershire
countycouncil

Appendix 1: Requests for information under FOI and EIR

Year	Measure	Adult Services	Children's Services / WCF	CIGT[2]	Commercial and Change	Economy & Infrastructure	Public Health	Total
2018/19	**No. of Requests**	139	318	296	323	438	36	**1550**
	Completed on time	91.4%	69.2%	88.9%	69.3%	94.1%	94.4%	**82.6%**
2019/20	**No. of Requests**	125	278	57	400	595	35	**1490**
	Completed on time	92.0%	86.7%	86.0%	82.5%	98.5%	80.0%	**90.5%**
2020/21	**No. of Requests**	135	203	38	337	545	41	**1482**
	Completed on time	92.5%	85.3%	86.4%	76.6%	97.5%	74.6%	**87.7%**
2021/22	**No. of Requests**	115	268	144	336	530	66	**1459**
	Completed on time	99.1%	89.9%	95.1%	86.1%	97.6%	93.9%	**93.2%**

Rather than record the actual time taken to complete requests as this can be difficult to do with any certainty when several people are involved in responses (including staff from CIGT, IACs and the actual business areas), requests are categorised into one of three categories of time taken to complete the request:

Year	Less than 5 hours	Between 5 and 15 hours	Over 15 hours	Total
2018/19	1334	177	39	**1550**
2019/20	1362	95	33	**1490**
2020/21	1273	142	67	**1482**
2021/22	1341	95	23	**1459**

[2] These are usually requests where the scope covers multiple Information Access Coordinators, where further information is required to enable us to process the request, or are for information about services not provided by the County Council e.g. bin collections

This page is intentionally left blank

worcestershire
countycouncil

CORPORATE AND COMMUNITIES OVERVIEW AND SCRUTINY PANEL 23 MAY 2022

THE COUNCIL'S IMPLEMENTATION OF MICROSOFT INTUNE (MOBILE DEVICE MANAGEMENT)

Summary

1. The Panel has requested information on the Council's implementation of Microsoft Intune (which is part of Microsoft EndPoint Manager).

2. Microsoft Intune is used by the Council to control how devices are used, including mobile phones, tablets, and laptops. It enforces a conditional access policy that ensures devices are compliant with the Government's security standards. Connectivity to council services e.g. email, OneDrive, MS Teams is no longer allowed from devices that are not verified as compliant with the Government's security standards.

3. The Cabinet Member with Responsibility for Corporate Services and Communication (CMR) and the Strategic Director of Commercial and Change have been invited to attend the meeting to respond to any questions from Panel members.

Background

4. The Council has sought to increase productivity of its workforce by enabling access to business email, calendar, and tasks from mobile devices. Whilst this was focused at corporately owned mobile devices, the previous implementation of this using Microsoft Exchange ActiveSync had resulted in any mobile device (including personal devices, subject to the use of a valid username/password) being able to connect and download Council data. Microsoft Exchange ActiveSync is a server technology not software that runs on the device in question. As such, prior to our implementation of Microsoft Intune, no software was installed on a device. This subjected the Council to several vulnerabilities as follows:

i. When a user leaves the Council, their account is disabled. However Worcestershire County Council (the Council) data on the mobile device was previously neither automatically nor manually wiped, as the only option available via Microsoft Exchange ActiveSync was the complete wipe of the mobile device resulting in the employee's personal data being destroyed as well as the corporate data. This meant that staff using personal mobiles who left had to choose to manually remove the Council's email data from the device. This almost certainly could have led to a data breach with non-Council staff having access to Council data that they shouldn't.

ii. Previously, the Council's mobile devices were, in general, not managed, for example having no mandated anti-virus/malware protection. Employees could

also choose to jailbreak[1] their mobile devices (to enable custom functionality), which is a practice that significantly increases the risk of malware. This could lead to data loss from an infected device.

5. In February, the Council underwent reaccreditation of Public Services Network (PSN) by the Government Digital Service (GDS). The position at the time was that the Council failed due to the current position on managing mobile phones; however, the pass was conditionally granted on the basis that the Council commit to implementing full conditional access of all mobile phones to corporate data by 30 April 2022. If the Council did not agree to this condition, then its PSN accreditation would be rescinded.

6. To mitigate these risks the Council implemented Microsoft EndPoint Manager (which brings together Microsoft Intune for cloud endpoint management and Microsoft Endpoint Configuration Manager for endpoints on-premises) supported by a Conditional Access Policy that enforces this for access to email from mobile devices. This will be further expanded to all services and all devices.

7. Connectivity to email is therefore no longer possible from devices that are not verified as compliant with the Government's security standards.

Mobile Device Management (MDM)

8. MDM is a proven methodology and toolset used to provide a workforce mobile productivity tools and applications while keeping corporate data secure.

9. The Council and its workforce rely on mobile devices such as smartphones, tablets and laptops for a wide assortment of tasks. However, because enterprise mobile devices access critical business data, they can threaten security if hacked, stolen or lost. So, the importance of managing mobile devices has evolved such that IT and security leaders now provision, manage and secure mobile devices within the corporate environment.

10. MDM is a solution that uses software as a component to provision mobile devices while protecting an organisation's assets, such as data. Organisations practice MDM by applying software, processes and security policies onto mobile devices and toward their use. Beyond managing device inventory and provisioning, MDM solutions protect the device's applications, data and content.

11. Microsoft EndPoint Manager, which includes Microsoft Intune, is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). It is used by the Council to control how devices are used, including mobile phones, tablets, and laptops. On personal devices, Microsoft Intune helps make sure the Council's data stays protected and can isolate council data from personal data.

Public Sector Network Compliance (PSN)

12. PSN compliance requires the Council to meet strict security standards when processing certain types of government data and accessing government systems. It is regularly audited, and the Council must annually report its security arrangements to the Cabinet Office. It is how the Council demonstrates that its security arrangement, policies

[1] To "jailbreak" means to allow an Apple phone's owner to gain full access to the root of the operating system and access all the features. Like jailbreaking, "rooting" is the term for the process of removing the limitations on a mobile or tablet running the Android operating system.

and controls are sufficiently rigorous for it to interact with the PSN and all those connected to it. It is good practice to apply the controls and methodologies to the whole Council and not just to services that utilise PSN associated systems or information. Penalties for non-compliance are that the Council would be restricted from accessing certain government systems and information.

13. Compliance with all the above standards assists the Council in keeping up to date with its security and cyber security policies and controls. This in turn ensures that Council systems and information are kept as secure as possible against emerging threats.

14. The PSN uses a walled garden[2] approach, which enables access to Internet content and shared services to be controlled. This is because the security of any one user connected to the PSN affects both the security of all other users and the network itself. The PSN compliance process exists to provide the PSN community with:

a. confidence that the services they use over the network will work without problems
b. assurance that their data is protected in accordance with suppliers' commitments
c. the promise that if things do go wrong, they can be quickly put right.

15. The direct implications of the Council not being accredited for PSN are:
    a. Access to CIS Searchlight[3] can only be obtained over the PSN network. CIS Searchlight is needed as part of the Blue Badge Service application process.
    b. Without Conditional Access and without PSN Accreditation the Council would NOT be able to connect the HSCN, as we would be unable to meet the requirements. This would prevent access to:
        - Integrated Care Record[4]
        - Carenotes[5]
        - EVIE[6]
        - Collaborate sharing with the NHS.
        - Prevent NHS obtaining access to Liquidlogic[7].
    c. Worcestershire Children First rely on PSN Accreditation to enable access to data controlled by Department for Education e.g. benefits.
    a. Access to the Health and Social Care Network (HSCN)[8] is dramatically made easier by having PSN Accreditation as it results in a significant number of questions not having to be answered.
    b. The Council relies on PSN Accreditation to support bids for funding/paid work.

[2] A walled garden is an software system wherein the service provider has control over applications, content, and/or media, and restricts convenient access to non-approved applicants or content.

[3] The Customer Information System (CIS) is used by the Department for Work and Pensions (DWP) to store information such as name, address, date of birth, National Insurance number.

[4] An Integrated Care Record (ICR) is a way of bringing together the various electronic records of a person's care. It takes information directly from existing systems used by health and social care organisations and presents it in a structured, easy-to-read format for health and care professionals.

[5] Carenotes is web-based child health, community & mental health system.

[6] Electronic View for Interoperable Exchange

[7] Liquidlogic's social care software

[8] The Health and Social Care Network (HSCN) is a data network for health and care organisations which replaced N3. It provides the underlying network arrangements to help integrate and transform health and social care services by enabling them to access and share information more reliably, flexibly and efficiently while benefiting from improved network and bandwidth capacity, financial savings and easier and smoother access to clinical systems.

Cyber Security

16. Throughout 2020 and into 2021, there was a significant and concerning increase in cyber-attacks, including ransomware attacks, on the public sector and education organisations. Ransomware is often used by cyber criminals in a way that doesn't initially target specific organisations. Once the malicious software is on a network, the criminals can monitor and control the encryption of data. Their aim is to encrypt, steal or leak data that will have the biggest impact on the organisation's services. The data held by these services is also at significant risk, including personal information (the electoral register), financial transactions (revenue and benefit payments), vulnerable people (adult social care), and school data (admissions, at risk children).

17. The Council has already invested in a range of measures to protect ~~our~~ systems and the data they hold from potential attacks. These include:

a. Implementing modern firewalls and scanning services.
b. Implementing infrastructure solutions to improve the resilience of services if, and when, a cyber-attack occurs.
c. Introducing training for the workforce and elected members.
d. Maintaining compliance with the PSN[9], PCI DSS[10], and DSPT[11] security standards, to retain secure inter-working and data sharing with public sector organisations.
e. Applying the government's cyber security guidance, 10 Steps to Cyber Security[12] and Cyber Essentials[13].
f. Carrying out ongoing health checks, penetration tests and cyber resilience exercises to test our systems and processes, e.g., Web Check[14].
g. Implemented Microsoft Office Protected View that opens Office documents in read-only mode with macros and other content disabled to reduce the risk of malware and other threats.
h. Working with partners across the public sector through participation in Cyber Security Information Sharing Partnerships[15], Warning, Advice and Reporting Points[16] and Local Resilience Forums[17] to protect our systems from, and put in place plans to respond to, cyber-attacks.

18. The priority is to ensure that the Council continues to be secure and resilient to cyber threats.

[9] Public Sector Network (PSN) (www.gov.uk/government/groups/public-services-network)

[10] Payment Card industry data Security Standards (PCI-DSS) PCI Security Standards Council Site

[11] Data Security and Protection Toolkit (DSPT) https://www.dsptoolkit.nhs.uk/

[12] 10 Steps to Cyber Security (10 steps to cyber security - NCSC.GOV.UK)

[13] Cyber Essentials (www.cyberessentials.ncsc.gov.uk)

[14] Web Check NCSC Web Check - NCSC.GOV.UK – a website configuration and vulnerability scanning service, developed with a number of public sector organisations including councils.

[15] Cyber Security Information Sharing Partnerships (CiSP) (www.ncsc.gov.uk/cisp),

[16] Warning, Advice and Reporting Points (WARPs) (www.ncsc.gov.uk/articles/what-warp)

[17] Local Resilience Forum (LRFs) (Local resilience forums: contact details - GOV.UK (www.gov.uk)

Data Security and Protection Toolkit (DSPT)

19. The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. This self-assessment tool enables the Council to demonstrate that it can be trusted to maintain the confidentiality and security of personal information, in particular health and social care personal records.

20. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

21. The criterion relating to Mobile Device Management in the 2021-2022 DSPT is:

If staff, directors, trustees and volunteers use their own devices (e.g., phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g., if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, then tick and write "Not applicable" in the comments box. A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices/)

22. The relevant BYOD[18] policy in the Council is the Communication and Mobile Devices Policy, and Microsoft Intune is the solution that the Council is using to enforce this.

The Council's Communication and Mobile Devices Policy

23. The purpose of the Communication and Mobile Devices Policy is to advise acceptable use with regard to mobile devices (including mobile phones) and communication systems used for business activities. With the convergence of data and voice and video communication systems, the ability to connect remotely to internal systems and the wide range of options offered by mobile devices, it is essential that these technologies be used by authorised persons for legitimate business activities.

24. Appendix 1 provides further information on the relevant clauses from the Communication and Mobile Devices Policy.

Benefits of Microsoft Intune

25. Secure solution for BYOD: Microsoft Intune provides a secure solution for BYOD as it ensures that the employee's device is appropriately configured to meet the

[18] Bring your own device (BYOD) refers to being allowed to use one's personally owned device, rather than being required to use an officially provided device.

Government's requirements to access corporate data. It provides this assurance by automatically assessing the configuration of the device against compliance policies without having any access to any data on the device.

26. Cost: Microsoft Intune is part of Microsoft Endpoint Manager, which is bundled with Microsoft 365. The Council has already invested in Microsoft 365 licenses and is therefore paying for Microsoft Intune. There are no additional licensing costs associated with the Council's use of Microsoft Intune.

27. Central management: Microsoft Intune can be used to provision, secure, manage and monitor all the Council's endpoints centrally in one system. This will accelerate the adoption of Zero Trust[19] and facilitate better security.

28. Increased productivity: With Microsoft Intune the time taken to provision new devices can be reduced, moving to greater automation in processes.

29. Improved cyber security: All endpoints can be secured, managed and monitored from a single system – Microsoft Intune. This will enable a consistent set of security policies, device management practices and compliance rules across all devices.

30. Improved Privacy for BYOD: Mobile security threats are rising and securing data on personal devices is paramount to good security and using devices for sensitive business such as banking makes security even more essential. Without security for personal smartphones, the Council is at risk of a breach.

31. Adherence to government requirements:
    a. Encryption: Checking data stored on the device is encrypted.
    b. Patching: Checking that the device and the version of operating system is still supported by the vendor and security updates are automatically applied.
    c. Authentication: Checking that the device meets minimum username / password requirements e.g. biometrics or PIN[20] or password complexity etc.
    d. Firewall: Checking the device has a working firewall if applicable.
    e. Anti-Virus / Anti-Malware: Checking that the device is protected from viruses and malware as applicable.
    f. Secured: Checking that the device hasn't been "jailbroken" thus ensuring that only trusted code can be executed on the device via applications installed via the official Google Play / Apple App Store.

Impact of Microsoft Intune on the owners of BYOD

32. If councillors and staff want to use their personal device to access council services, then they must ensure the device is enrolled in Microsoft Intune and meets the Council's compliance requirements. Connectivity to council services e.g. email, OneDrive, MS Teams is no longer allowed from devices that are not verified as compliant with the Government's security standards.

[19] Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

[20] A personal identification number (PIN), or sometimes redundantly a PIN number or PIN code, is a numeric (sometimes alpha-numeric) passcode used in the process of authenticating a user accessing a system. In mobile devices, the PIN acts like a password preventing other people from gaining unauthorized access to the device. This is a numeric code which must be entered each time the device is started (unless the PIN security feature is turned off).

33. Failure to meet the Government's security requirements will automatically result in access to council services on personal devices being blocked.

34. By enrolling their mobile device into Microsoft Intune, IT will be able to take the following actions on their phone or tablet to make sure council information is secure. These actions would only be undertaken following consultation with the device owner.

a. Reset the phone to factory settings if it is lost or stolen.
b. Remove company-related files and apps (without removing personal files or apps).
c. Require the use of a password or PIN.
d. Remotely reset the PIN or lock the phone or tablet if it is lost or stolen.
e. Make the phone or tablet compatible with the Council's security standards, which helps the individual as well as the company.

35. Once the device is enrolled, IT will be able to see this type of information on the phone or tablet:

- Owner
- Model
- Device name
- Operating system
- Serial number
- Council apps
- Manufacturer

36. IT will not be able to see this type of information on the phone or tablet:

- Call history
- Location
- Text messages
- Camera roll
- Personal email
- Contacts and calendar
- Personal data
- Web history
- Personal apps

Impact of resetting a device to factory settings

37. IT and Digital will only reset devices to factory settings if required by the owner of the device, and in the eventuality that the device is lost or stolen. It should be noted that there are no risks of damage to the device associated with factory resetting a smartphone.

38. Factory reset also known as master reset, hard reset or hardware reset is a built-in feature for electronic devices. A factory reset erases all data, settings and applications stored on the device. It returns the smartphone to the condition it was when it was brand new.

39. Irrespective of any enrolment with Microsoft Intune, device owners can perform a factory reset themselves on their device. In addition, they can restore and recover their backed-up data after a factory reset. Most services have some form of cloud backup, for example via a Google account for Android, or iCloud for Apple users. It should be noted that there are benefits that may be achieved from a factory reset of an Android or iPhone:

i. Improves Smartphone Performance: The longer smartphones are used, the more unnecessary data it accumulates. There is also the leftover data from uninstalling apps. This data consumes a lot of storage and memory in the background and tends to slow the device down. By factory resetting, the accumulated clutter is removed. The smartphone then becomes responsive and fast as when it was brand new and is potentially a way to improve smartphone's system performance.

ii. Factory reset serves as a last resort method in solving certain serious smartphone problems. It might be that the device is stuck at starting or a malicious is causing phones issues (crashes, freezing, poor performance etc.). These problems can make it difficult to use the phone or access it at all. By resetting it to factory settings it is possible to get rid of the problem.

Impact of resetting a Personal Identification Number (PIN) on a BYOD

40. There are no risks to personal devices associated with the reset of a PIN.

41. PINs would not be reset by the Council unless specifically requested by the owner of the BYOD.

42. If the owner of a BYOD had forgotten their pin / passcode, then the Council could be contacted to reset their PIN so they could access their device again.

43. In the extremely unlikely scenario that a PIN had accidently been reset without the authorisation of the owner of the device, then the Council could be contacted to reset the PIN again so the owner could access the device.

Mobile management solutions from multiple organisations

44. In a scenario where the MDM solution from another organisation has caused a technical issue with the Council's use of Microsoft Intune on a BYOD, then the IT department would liaise with the device owner and potentially the other organisation to try to resolve any technical issue.

45. If the other organisation is using Microsoft Intune (which is becoming increasingly likely due to the costs of Microsoft Intune being part of the Microsoft 365 E3 license), Microsoft potentially provide a resolution to this as per the article below. Whilst, this functionality is still in preview, it should enable the Council to trust the MDM solution of the other organisation thus enabling scenarios where devices managed by a district council, for example, can be trusted to connect to the County Council's services.

Cross-tenant access overview - Azure AD | Microsoft Docs

Financial implication to the Council

46. Microsoft Intune is part of Microsoft Endpoint Manager, which is bundled with the Council's Microsoft 365 licences. The Council has already invested in Microsoft 365 licenses and is therefore already paying for Microsoft Intune.

47. If councillors and staff choose to access council services from a personal device, they will be required to voluntarily enrol into Microsoft Intune and meet the Council's compliance requirements before access to council services are granted. There is no financial implication to the council in this scenario.

48. The Council can provide a corporate smartphone to officers and Councillors, which will be enrolled in Microsoft Intune to ensure it meets compliance requirements. The standard smartphone currently issued is the Samsung Galaxy A13, at a cost of £139 per handset plus the monthly contract.

Communications to staff and Members

49. The implementation of Microsoft Intune has been communicated to staff and councillors. Information has been provided on the Council's intranet (OurSpace) and several emails have been issued, as well as information within the Microsoft Intune guidance documentation. The communications explain the purpose of Microsoft Intune, what the software enables IT to do on personal devices, and what information is and isn't accessible.

50. Self-service instructions on how to enrol into Microsoft Intune have been provided.

51. During the enrolment process information is provided to explain what information the Council will be able to see, what can't be seen, as well as the actions that the Council will be able to perform on the BYOD.

Options available to staff and councillors

52. The use of personal devices is absolutely an individual decision for each member of staff and councillors to make themselves, and the Council does not mandate that they do so.

53. Therefore, if councillors and staff wish to access council services from a mobile device, they have the following choice:

i. Via a Personal device: Personal devices will need to be voluntarily enrolled into Microsoft Intune and meet the Council's compliance requirements before access to council services are granted.
ii. Via a Council device: The Council will provide a corporate smartphone, which will be enrolled in Microsoft Intune to ensure it meets compliance requirements.

Purpose of the Meeting

54. The Panel is asked to consider the information provided and:

- determine any comments to make to the Cabinet Member with Responsibility for Corporate Services and Communication

- agree whether any further Scrutiny is required at this stage.

Supporting Information

- Appendix 1: Communication and Mobile Devices

Contact Points

Andrew Spice, Strategic Director of Commercial and Change
Telephone: 01905 846678
Email: aspice@worcestershire.gov.uk

Sandra Taylor, Assistant Director for IT and Digital
Telephone: 01905 845447
Email: staylor12@worcestershire.gov.uk

Emma James / Jo Weston, Overview and Scrutiny Officers
Telephone: 01905 844964
Email: scrutiny@worcestershire.gov.uk

Background Papers

In the opinion of the proper officer, in this case the Assistant Director for Legal and Governance there are no background papers relating to the subject matter of this report:

All agendas and minutes are available on the Council's website here.

worcestershire
countycouncil

Appendix 1: Communication and Mobile Devices

The Communication and Mobile Devices (User Policy) provides the following guidance for users:

6.3	**Bring Your Own Device**
6.3.1	Personally owned communication devices may not be connected to or synchronised with the Council's computer systems or networks unless approved by the Assistant Director for IT and Digital and the device owner agrees to the security requirements regarding the management of the device. BYOD security requirements include: • Agreement that the device will be managed by the Council • Agreement for the Council security profile to be applied to the device **Explanation** the Council must be able to protect its IT resources and in order to do this it must be able to apply specific security settings and limit the functionality of the device. One of the biggest threats to corporate IT security is the portable device which is periodically connected to the corporate network as this may potentially introduce viruses and other malware and aid information leakage. Portable devices owned personally by staff or contractors may not always have the tightest security as this often impacts on functionality, e.g., password or pin protection. The Council must be able to ensure that every device connected to the computer system and/or network has the same configuration and security settings applied and therefore the level of risk is mitigated.
6.3.2	The Council corporate data and the management application must be removed and the user may be required to bring their device in for this to be achieved. **Explanation** As potentially confidential information could be stored on the device (e.g. email) the Council must ensure it is protected to the level of its sensitivity. This requirement relates to devices supplied by the Council or to a personally owned device supplied by a user. Security settings may include: • PIN or Password Protection • Autolock • Anti Virus installed where available • Personal firewall installed where available • Encryption turned on • Certificates installed • Disabling non-essential communications functionality • Limiting applications to those required for business purposes (e.g. disable Apps Store, Camera, iTunes, Cloud Storage Services, YouTube etc) • The ability to remote wipe the device
6.3.3	Maintenance responsibilities for mobile devices used for business purposes are as follows: • the Council owned and supplied devices will be fully maintained by the Council

	• Personally owned devices will be managed by the Council but maintained by the user Any issues must be logged with myIT Support. **Explanation** This requirement clearly defines who is responsible for devices and their maintenance. the Council will not be responsible for damage to, or loss of information incurring on personally owned devices under any circumstances. Maintenance means keeping the operating system up to date and ensuring that the device remains operational. With the development of malware designed specifically to infect mobile devices it is essential that these devices have the latest versions of operating systems installed and other protection mechanisms such as anti-virus and a personal firewall if available. Just like any other virus infection, infected devices will spread the virus to other devices and could potentially affect the computing environment itself if a direct connection can be made between the device and the internal computer network.

The Communication and Mobile Devices (Technical Policy) provides the following technical guidance:

Mobile Device Management

6.2.1	A risk assessment must be carried out by the Assistant Director for IT and Digital to confirm that mobile devices and communications systems do not create additional security vulnerabilities which are unacceptable to the Council. Managers may only approve devices that have been evaluated and approved as risk free by the Assistant Director for IT and Digital. **Explanation** The Assistant Director for IT and Digital must be satisfied that the increased automation and functionality offered by the introduction of mobile devices and communications systems is warranted when compared with the additional security threats that they introduce into the computing environment. He or she must also ensure that any device offered to a staff member is configured with the appropriate security settings and that the threat of information leakage or interception is minimised.
6.2.2	Mobile devices connecting or synchronising to the Council's computing resources must be configured with the Council security profile which may include: • Passwords or Pin numbers • Autolock • Remote Wipe • Disabling applications or functions that are not required for business purposes • Encryption and digital certificates where information is considered sensitive or confidential • Sandboxing or a no data at rest configuration • Anti Virus • Firewall

	• Device identification • Auto update of the operating system for patches and system upgrades In a BYOD situation, the user must agree to have the device managed by the Council who will ensure that it is patched and can be wiped if lost or stolen. **Explanation** Although many users will not consider a tablet or mobile phone to be a security threat to the Council, the ability to access email, customer address lists and other corporate information remotely does create security vulnerabilities if devices are not configured with the appropriate security settings. The security profile must be enforced on devices that are to be connected to the corporate network. Users are not permitted to change these settings.

This page is intentionally left blank