ADUR & WORTHING
COUNCILS

Joint Staff Committee
29 March 2023
Agenda Item 9

Key Decision: No

Ward(s) Affected:

Blended Working Policy

Report by the Director for Digital, Sustainability and Resources

Executive Summary

1. **Purpose**

1.1 The report seeks the changes to the Adur & Worthing Councils Blended Working Policy to be noted.

1.2 The aim of the policy is to enable staff to voluntarily work a proportion of their working hours from home, where their role is deemed by their manager as suitable.

2. **Recommendations**

2.1 The Joint Staff Committee is recommended to note the changes to the Blended Working Policy with an implementation date of immediate effect.

2.2 The changes have been agreed by the Head of Human Resources, in consultation with the Chief Financial Officer and the Head of Legal Services, as these changes are deemed as minor and non-consequential amendments to the Policy, under the delegated authority given to them by the Joint Staff Committee.

3. **Context**

3.1 The Blended Working Policy has been updated to ensure that it is in line with the Adur and Worthing Councils' Information Security Policy.

4. **Issues for consideration**

4.1 Whilst the essence of the Blended Working Policy is to enable staff to voluntarily work from home for a proportion of their working hours, they are expected to maintain the same standards of security of information, system security and security of equipment regardless of their location of work. This includes the Councils' policies on the Data Protection Act, GDPR and the Freedom of Information Act.

4.2 All the changes to the policy are in section 10 and are also summarised on Appendix

5. **Engagement and Communication**

5.1 Unison have been consulted with and have agreed the changes.

6. **Financial Implications**

6.1 There are no financial implications arising from the update of this policy.

7. **Legal Implications**

7.1 There are no legal implications due to the changes being made to this policy.

7.2 This policy is not contractual and does not form part of the terms and conditions of employment.

7.2 Section 112 Local Government Act 1972 gives the Council the power to appoint staff on such terms and conditions as it considers appropriate.

Background Papers

- Summary of changes to the policy as Appendix 1
- Amended Adur & Worthing Councils' Blended Working Policy available at Appendix 2
- Previous Adur & Worthing Councils' Blended Working Policy available at Appendix 3
- Adur & Worthing Councils' Information Security Policy available at Appendix 4
- Blended Working Policy Equality Impact Assessment (EIA) available at Appendix 5

Officer Contact Details:-

Heidi Christmas

Head of Human Resources
Worthing Town Hall
Direct Dialling No 01903 221183
Email:heidi.christmas@adur-worthing.gov.uk

Sustainability & Risk Assessment

1. Economic

The proposed policy will enable the Councils to provide services in a more flexible and efficient way.

2. Social

2.1 Social Value

Matter considered and no issues identified

2.2 Equality Issues

The Equality Impact Assessment for this policy and associated statistics are attached as Appendix 2

2.3 Community Safety Issues (Section 17)

Matter considered and no issues identified.

2.4 Human Rights Issues

The proposal for staff to work from home is on a voluntary basis, so if there are staff members that don’t want to work from home for any reason then they can work at their contractual base.

3. Environmental

Staff working from home for a proportion of their working hours may decrease the number of journeys they are making to and from work, which in turn could reduce the amount of CO2 emissions.

4. Governance

DSE Workstation assessments are covered in the policy and the stance is that if a staff member’s working environment does not meet the DSE workstation standards they may be unable to work safely from home and then will need to work in the office.

Current		Proposed		Information Security Policy references...
10.1 ICT policies apply to all employees, wherever they may be working. Employees are expected to maintain the same standards of security of information, system security and security of equipment regardless of their location of work. This includes the Councils' policies on the Data Protection Act , GDPR and the Freedom of Information Act.		10.1 ICT policies apply to all employees, wherever they may be working. Employees are expected to maintain the same standards of security of information, system security and security of equipment regardless of their location of work. This includes the Councils' policies on the Data Protection Act , GDPR and the Freedom of Information Act. All employees must make themselves familiar with and abide by the terms of the Information Security Policy (LINK).		NA
10.2 Employees who transport equipment (e.g. laptops, mobile phones) should not, as far as practicable, leave this unattended in vehicles.		*Remove as duplicated in Information Security Policy*		Points 8. Security of Equipment and 10. Security and Storage of Information
10.3 The employee must not allow members of their household or third parties to access or use any Councils equipment.		*Remove as duplicated in Information Security Policy*		Point 16. and under Annex A - Remote Working 1.1
10.4 Employees who work from home are responsible for keeping all documents and information associated with the Councils secure and confidential at all times. This includes destroying confidential documents appropriately.		*Remove as duplicated in Information Security Policy*		8. Security of Equipment and 13. Retention and Disposal of Information
10.5 Employee's should not print documents off at home.		*Remove as duplicated in Information Security Policy*		12. Information Sharing and Distribution, though I have made a suggesting it includes the word "home"
10.6 An employee should take the appropriate steps when dealing with confidential matters from home. Where possible, they should ensure they are working in a confidential work space and if taking a confidential call they should wear a headset to mitigate any risk of confidential information being overheard.		10.2 All employees should take the appropriate steps when dealing with confidential matters in all locations, including non office sites. Where possible, they should ensure they are working in a confidential work space where documents, including those on screen, cannot be viewed by others, and if taking a confidential call they should wear a headset to mitigate any risk of confidential information being overheard.		

ADUR & WORTHING
COUNCILS

Blended Working Policy

1.0 Overview

1.1 This policy applies to all employees of Adur and Worthing Councils, it also applies to temporary workers, agency staff and contractors. It sets out the standards for working arrangements to benefit the Councils, their employees and customers. (Referred to hereafter as employees)

1.2 This policy has been developed from a position of trust acknowledging that all staff members work hard and our ways of working should support us in achieving the best outcomes for the residents of Adur and Worthing.

1.3 This policy should be interpreted in accordance with the Equalities Act 2010 and shall be applied fairly and consistently to all employees in roles identified as suitable for blended or home working.

1.4 The Councils promote a blended working approach and agree to an employee voluntarily working a proportion of their working hours from home, where their role is deemed by their manager as suitable. In some instances, where the role permits, the Councils may agree to an employee working 100% of their working hours at home.

1.5 Every job is different and therefore the Councils are unable to agree that all roles will have this level of flexibility.

1.6 This policy will be reviewed on an ongoing basis and it is anticipated to be reviewed after 12 months, notwithstanding exceptional circumstances. The Councils reserve the right to amend or remove this policy and return everyone to the office, following normal consultation processes.

2.0 Guiding Principles

2.1 The following guiding principles are how we want to work with our teams across the Councils:

● Our ways of working will ensure we provide the high quality service to our communities, e.g. in terms of service standards and accessibility (in line with Good Services)

● Our focus is on delivering the best outcomes

● The work environment needs to be conducive to carry out the role

● Our workforce is flexible in terms of work location and hours subject to service needs, agreed in Team Charters

● The office is the formal work location, unless otherwise agreed.

● To enable working from flexible locations, teams and individuals will proactively engage and communicate

- Staff may be required to change their work location to meet the requirements of their role, this may be at short notice in the case of an emergency or for business continuity reasons.

- All work environments need to be safe (including DSE, data security, personal security, infection control)

3.0 Definition of Blended Working

3.1 This is where an employee will work a proportion of their time in the office and a proportion of their time at home. Their work base location will remain as the office.

3.2 This will be a blended working approach, where the employee may agree with their line manager on a weekly basis. The days of the week and work pattern may vary and depend on the needs of the business.

3.3 The employee should attend the office at the request of the manager for meetings, team activity, general work days, training and to assist with coaching of other team members.

3.4 The role will be assessed by the manager and the job description/person spec updated to reflect the ability to work from home on an occasional basis.

4.0 Definition of Homeworkers

4.1 Where it is agreed that an employee may work home for 100% of their working week, their work base location will be ‘home’ and this will be reflected in their statement of terms and conditions of employment.

4.2 The employee may be required, at reasonable notice to the office at the request of the manager for meetings, team activity, general work days, training and to assist with coaching of other team members.

4.3 The role will be assessed by the manager and the job description/person spec updated to reflect the ability to work from home on a full time basis.

5.0 Roles and responsibilities

5.1 **Managers** will use the following to decide the level of blended working possible for the roles within their teams:

<u>The role:</u>

- The role and team has successfully worked from home during lockdown

- The quality of the teams work has not been affected by working remotely

- Level of service has been maintained through remote working during lockdown

- The team can be managed by outcomes

- The team is able to work together remotely and does not require day to day supervision

- The role does not have duties requiring it to attend an office i.e. staffing reception, scanning, fixing equipment etc.

The person:

- they have a suitable home working environment that meets the DSE workstation assessment requirements
- their organisational and time-management skills
- their ability to work without constant direct supervision
- their ability to cope with conflicting priorities work/homelife balance

5.2 Manager Responsibility to

- Work with the their employees and identify the roles that are able to work from home
- Manage their teams to ensure they meet their productivity targets and objectives
- Understand where their team is on a daily basis
- Have regular 1:1s with individuals (at least every six weeks) to discuss performance and wellbeing
- Hold regular team meetings and gather their team together in person when required
- Ensure the employee has the appropriate equipment to enable them to do their job effectively
- Ensure the job description is updated to reflect the blended working approach
- Regardless of work location, give the team regular feedback and put in place ways of communicating with them (e.g. bulletins, team briefs, team meetings).
- Monitor the hours their team work to ensure they comply with working time regulations.
- Ensure all their team have completed a DSE workstation assessment.
- Ensure IT kit is returned to the IT team when a member of staff leaves their team or the organisation ensuring that document ownership is correctly reallocated.
- Determine and review working patterns and practices in the team with fairness.
- Ensure work styles and practices are used to enhance business performance.

5.3 Employee Responsibility to

- Ensure their space when working from home is free from distractions where possible
- Ensure they have an appropriate place to work with the correct equipment and compliant with DSE workstation assessment requirements
- Attend the office as required by their manager and for any activity required to fulfil their job role (i.e. for training, meetings where they are requested to attend in person, to get support if there are any performance concerns raised, or to participate in team activities)
- Keep in touch with their line manager and their colleagues as they would in the office
- Meet any objectives and targets set
- Take care of their health, making sure they have completed an annual DSE workstation assessment if they are working from home

● Be contactable via phone or email, when working regardless of their place of work.

● Ensure their contact details are up-to-date on the staff directory and in their email signature, including mobile phone numbers where applicable.

● Keep calendars up-to-date with location and meeting details.

● Attend meetings, training and provide office cover where needed.

● Abide by data protection and GDPR, freedom of information and IT policies and take all steps possible to ensure confidentiality regardless of where they work.

6.0 Base Location

6.1 Blended Working

6.1.1 The work base location for blended working will be the employee's contractual work base.

6.1.2 Should the employee be required to attend the office at any time due to issues with equipment or technology the employee must be available to do so at reasonable notice.

6.1.3 Travelling time to and from the work base office to home location and vice versa, is not classed as working hours.

6.1.4 The employee will be able to claim travel expenses from where they are working on that day, please refer to the Staff Expenses & Reimbursements Policy.

6.2 Home Working

6.2.1 The work base location for a 'home worker' will be the employees' home address and this will be reflected in their contract.

6.2.2 The employee may be requested to attend meetings but reasonable notice must be provided.

6.2.3 Travelling time to and from their 'home base' to the office is classed as working hours and may be expensed, please refer to the Staff Expenses & Reimbursements Policy.

7.0 Hours of Work

7.1 The employee will work their contractual hours of employment. However, where the role permits the employee will not be subject to any fixed hours, and is free to perform their duties at work times to suit as long as they meet their required outcomes and deadlines and are available as per the job description.

7.2 The employee must keep their manager informed of their working pattern for the week and ensure that they are meeting their job description and fulfilling their statement of terms and conditions of employment.

7.3 The employee must comply with the Working Time Regulation Act 1998.

8.0 Equipment

8.1 All employees that work from home, for any part of their working hours, are expected to provide an appropriate office environment, with a suitable desk and chair in line with the DSE Workstation Assessment.

8.2 It is the Councils’ policy to provide and maintain all equipment and materials necessary for you to work from home in line with the following equipment guideline below.

Item	Blended Worker	Homeworker
Laptop	Y	Y
Laptop Stand	DSE Assessment	DSE Assessment
Screen	Y	Y
2nd Screen	Role dependent	Role dependent
Keyboard	Y	Y
Wrist Rest	DSE Assessment	DSE Assessment
Mouse	Y	Y
Foot rest	DSE Assessment	DSE Assessment
Desk	Y - dependent on % of time worked	Y
Office Chair	Y - dependent on % of time worked	Y
Printer	N	Y - dependent on business need
Shredder **Lockable Cabinet** **Laptop Rucksack/Bag** **Trolley Bag**	N N Y Role Dependent	Y - dependent on business need Y- dependent on business need Y Role Dependent

8.3 The Manager will discuss equipment with employees on an individual basis based on their job role, the number of days working from home and the completed DSE Assessment.

8.4 It is the employee’s duty to ensure that proper care is taken of such equipment and materials as they remain the property of the Councils.

8.5 Should the employee not have the right equipment or environment, the manager may request that the employee returns to their main base in line with their contracted hours.

8.6 On termination of employment for any reason, the employee will be required to return all equipment that has been provided to their work base.

8.7 The employee will sign an inventory of items that will be maintained on their file.

9.0 DSE Workstation Assessments

9.1 Line managers have a responsibility to ensure that a health and safety risk assessment is undertaken for each employee in relation to the work-style, practices and location of their work.

9.2 Where employees are visiting clients/sites etc., the line manager and individual must ensure that an appropriate lone working risk assessment is undertaken and appropriate measures implemented in line with the Councils' Lone Working Policy.

9.3 The employee must complete an annual DSE workstation assessment for the home and the office. The employee is responsible for ensuring their workstation is in line with the provided guidelines and that they produce their equipment for annual PAT testing in line with the Councils' processes.

9.4 If the employee's home working environment does not meet the required DSE Workstation assessment standards they may be unable to work safely from home, and they will need to work in the office.

9.5 Employees have a responsibility for implementing any actions identified in order to reduce/mitigate risks to make their work environment safe. The line manager should take reasonable steps to ensure the employee has implemented any actions identified.

9.6 Line managers have a responsibility to ensure that their team members carry out a DSE Workstation assessment, on their home working setup and/or their office base.

9.7 Line managers should review health and safety on a regular basis and it should be discussed frequently during one to one meetings. Where there are concerns, appropriate advice should be sought. This may include employees being assessed by a trained workstation assessor to outline specific equipment needed (e.g. special computer mouse, or a specific type of chair).

9.8 For any accidents that occur in the workplace (which includes the home or any temporary workplace if the accident is work related), the employee should report this to their manager who will complete an accident book report as soon as reasonably practicable and in any case by the end of the current working day. In these circumstances, the line manager should inform the Safety and Resilience team immediately and (if this was not done at the time of the injury) complete an Incident Report Form based on the information given.

10.0 Security and Confidentiality

10.1 ICT policies apply to all employees, wherever they may be working. Employees are expected to maintain the same standards of security of information, system security and security of equipment regardless of their location of work. This includes the Councils' policies on the Data Protection Act, GDPR and the Freedom of Information Act. All employees must make themselves familiar with and abide by the terms of the Information Security Policy.

10.2 All employees should take the appropriate steps when dealing with confidential matters in all locations, including non office sites. Where possible, they should ensure they are working in a confidential work space where documents, including those on screen, cannot be viewed by others, and if taking a confidential call they should wear a headset to mitigate any risk of confidential information being overheard.

11.0 Working Environment

11.1 It's important that staff are able to concentrate on their work and maintain their productivity levels, and distractions kept to a minimum, ie. such as ensuring suitable arrangements for children and dependents is in place.

11.2 Should you require to take leave to look after your dependents more information is available in Section 7: Special Paid Leave within the Leave Policy.

12.0 Stationery and Sundries

12.1 The employee will be expected to order their stationery and sundries from their work location as per the normal procedures. The employee is permitted to take this stationery home for use for work purposes.

13.0 Home domestic bills

13.1 The employee will be expected to pay the costs of all their personal domestic bills. Costs towards household bills, such as gas, water and electricity will not be reimbursed.

14.0 Telephone and Internet Access

14.1 The employee will be expected to pay the costs of all personal telephone and internet connections into their home.

14.2 The employee should not use their personal mobile or phone line for business phone calls.

15.0 Insurance and liability

15.1 The employee is responsible for checking that all home and content insurance policies provide adequate cover for the fact they are working from home.

15.2 Employees are covered by the Councils' insurance policy for employer's liability and personal accident in the same way whether they are office based employees or not.

15.3 Equipment supplied to flexible/mobile workers is covered by the Councils' insurance arrangements, providing it is used for work purposes only, and in line with the manufacturer's instructions.

15.4 It is the responsibility of those who work from home to contact their own insurance company, landlord and/or mortgage provider to advise that they will be working from home.

15.5 The Councils will not reimburse any increase in insurance premium.

16.0 Work Deliverables

16.1 The employee will be measured on outcomes and will be monitored by their line manager. Should an employee complete their allocated workload prior to the end of the daily contracted hours, they must request more work.

17.0 Probation Period

17.1 Any employee who is starting a new role with the Councils may be required to attend the office for training purposes for an intensive period of time before shifting to blended working. This will be agreed with the employee prior to commencement in the role and may vary on a role to role basis.

18.0 Staying in touch

18.1 It is important for the employee to stay in contact with their team and manager on a regular basis.

18.2 The Councils will encourage all employees whether in blended working or home working to attend the office with their colleagues regularly for meetings, training or general work purposes.

18.3 Employees working in a blended work pattern, should at the request of their manager attend the workplace at short notice in the case of an emergency or for business continuity reasons. This will be role dependent.

19.0 Performance

19.1 The manager will have regular 1:1 meetings with their team members to ensure performance is to the required standard and is meeting the manager's expectations. 1:1s are encouraged to happen in person whenever possible.

19.2 Should the employees' performance be affected in any way, the manager will commence the normal performance management process as detailed in the Performance Support Policy.

19.3 The manager has the right to request that the employee attends the office on a more regular basis during any period of performance management, to enable support and coaching. This may be up to 5 days a week or in line with the employee contractual working pattern.

20.0 Training and Development

20.1 Should an employee require support in their role, they must raise this with their line manager. This could happen as part of the regular 1:1 conversations that a member of staff has with their line manager

21.0 Disciplinary or Grievance

21.1 The Councils' normal disciplinary and grievance procedure will apply. Should you be required to attend a meeting in relation to either of these procedures you will be expected to attend the meeting at a Councils' premises.

22.0 Visits to the employees' home

22.1 Should the Councils have concerns relating to Health and Safety matters they may request an appointment to conduct an assessment at the employees home. Such appointments will be arranged at a mutually convenient time.

23.0 Dispute Resolution

23.1 Should there be a dispute between the employee and the manager, they should ideally try and resolve it between them informally. If this is not possible then this should be escalated in the first instance to the Head of Service for resolution.

23.2 Should the situation not be resolved within the as per 23.1, then HR should be contacted and then the normal grievance procedure must be followed.

24.0 Failure to comply with this policy

24.1 Failure to comply with any of this policy may result in the employee returning to the office full time and/or appropriate performance management/disciplinary processes being applied.

25.0 Policy Implementation & Monitoring

25.1 Responsibility for the implementation, monitoring and development of this policy lies with the Head of Human Resources and CLT.

25.2 Day to day operation of the policy is the responsibility of managers' who will ensure that this policy is adhered to.

Date policy agreed with Unison: 4th August 2021

Date agreed by Joint Staff Committee: 29th September 2021

Date policy formally adopted: 1st November 2021

Date for review: 1 year from formal adoption of policy 31st October 2022

Policy reviewed and non consequential changes agreed: 16th November, 2022

ADUR & WORTHING
COUNCILS

Blended Working Policy

1.0 Overview

1.1 This policy applies to all employees of Adur and Worthing Councils, it also applies to temporary workers, agency staff and contractors. It sets out the standards for working arrangements to benefit the Councils, their employees and customers. (Referred to hereafter as employees)

1.2 This policy has been developed from a position of trust acknowledging that all staff members work hard and our ways of working should support us in achieving the best outcomes for the residents of Adur and Worthing.

1.3 This policy should be interpreted in accordance with the Equalities Act 2010 and shall be applied fairly and consistently to all employees in roles identified as suitable for blended or home working.

1.4 The Councils promote a blended working approach and agree to an employee voluntarily working a proportion of their working hours from home, where their role is deemed by their manager as suitable. In some instances, where the role permits, the Councils may agree to an employee working 100% of their working hours at home.

1.5 Every job is different and therefore the Councils are unable to agree that all roles will have this level of flexibility.

1.6 This policy will be reviewed on an ongoing basis and it is anticipated to be reviewed after 12 months, notwithstanding exceptional circumstances. The Councils reserve the right to amend or remove this policy and return everyone to the office, following normal consultation processes.

2.0 Guiding Principles

2.1 The following guiding principles are how we want to work with our teams across the Councils:

- Our ways of working will ensure we provide the high quality service to our communities, e.g. in terms of service standards and accessibility (in line with Good Services)
- Our focus is on delivering the best outcomes
- The work environment needs to be conducive to carry out the role
- Our workforce is flexible in terms of work location and hours subject to service needs, agreed in Team Charters
- The office is the formal work location, unless otherwise agreed.
- To enable working from flexible locations, teams and individuals will proactively engage and communicate
- Staff may be required to change their work location to meet the requirements of their role, this may be at short notice in the case of an emergency or for business continuity reasons.
- All work environments need to be safe (including DSE, data security, personal security, infection control)

3.0 Definition of Blended Working

3.1 This is where an employee will work a proportion of their time in the office and a proportion of their time at home. Their work base location will remain as the office.

3.2 This will be a blended working approach, where the employee may agree with their line manager on a weekly basis. The days of the week and work pattern may vary and depend on the needs of the business.

3.3 The employee should attend the office at the request of the manager for meetings, team activity, general work days, training and to assist with coaching of other team members.

3.4 The role will be assessed by the manager and the job description/person spec updated to reflect the ability to work from home on an occasional basis.

4.0 Definition of Homeworkers

4.1 Where it is agreed that an employee may work home for 100% of their working week, their work base location will be 'home' and this will be reflected in their statement of terms and conditions of employment.

4.2 The employee may be required, at reasonable notice to the office at the request of the manager for meetings, team activity, general work days, training and to assist with coaching of other team members.

4.3 The role will be assessed by the manager and the job description/person spec updated to reflect the ability to work from home on a full time basis.

5.0 Roles and responsibilities

5.1 **Managers** will use the following to decide the level of blended working possible for the roles within their teams:

The role:

- The role and team has successfully worked from home during lockdown
- The quality of the teams work has not been affected by working remotely
- Level of service has been maintained through remote working during lockdown
- The team can be managed by outcomes
- The team is able to work together remotely and does not require day to day supervision
- The role does not have duties requiring it to attend an office ie. staffing reception, scanning, fixing equipment etc

The person:

- they have a suitable home working environment that meets the DSE workstation assessment requirements
- their organisational and time-management skills
- their ability to work without constant direct supervision
- their ability to cope with conflicting priorities work/homelife balance

5.2 **Manager Responsibility to**

- Work with the their employees and identify the roles that are able to work from home
- Manage their teams to ensure they meet their productivity targets and objectives

- Understand where their team is on a daily basis
- Have regular 1:1s with individuals (at least every six weeks) to discuss performance and wellbeing
- Hold regular team meetings and gather their team together in person when required
- Ensure the employee has the appropriate equipment to enable them to do their job effectively
- Ensure the job description is updated to reflect the blended working approach
- Regardless of work location, give the team regular feedback and put in place ways of communicating with them (e.g. bulletins, team briefs, team meetings).
- Monitor the hours their team work to ensure they comply with working time regulations.
- Ensure all their team have completed a DSE workstation assessment.
- Ensure IT kit is returned to the IT team when a member of staff leaves their team or the organisation ensuring that document ownership is correctly reallocated.
- Determine and review working patterns and practices in the team with fairness.
- Ensure work styles and practices are used to enhance business performance.

5.3 **Employee Responsibility to**

- Ensure their space when working from home is free from distractions where possible
- Ensure they have an appropriate place to work with the correct equipment and compliant with DSE workstation assessment requirements
- Attend the office as required by their manager and for any activity required to fulfil their job role (i.e. for training, meetings where they are requested to attend in person, to get support if there are any performance concerns raised, or to participate in team activities)
- Keep in touch with their line manager and their colleagues as they would in the office
- Meet any objectives and targets set
- Take care of their health, making sure they have completed an annual DSE workstation assessment if they are working from home
- Be contactable via phone or email, when working regardless of their place of work.
- Ensure their contact details are up-to-date on the staff directory and in their email signature, including mobile phone numbers where applicable.
- Keep calendars up-to-date with location and meeting details.
- Attend meetings, training and provide office cover where needed.
- Abide by data protection and GDPR, freedom of information and IT policies and take all steps possible to ensure confidentiality regardless of where they work.

6.0 Base Location

6.1 Blended Working

6.1.1 The work base location for blended working will be the employee’s contractual work base.

6.1.2 Should the employee be required to attend the office at any time due to issues with equipment or technology the employee must be available to do so at reasonable notice.

6.1.3 Travelling time to and from the work base office to home location and vice versa, is not classed as working hours.

6.1.4 The employee will be able to claim travel expenses from where they are working on that day, please refer to the Staff Expenses & Reimbursements Policy.

6.2 Home Working

6.2.1 The work base location for a 'home worker' will be the employees' home address and this will be reflected in their contract.

6.2.2 The employee may be requested to attend meetings but reasonable notice must be provided.

6.2.3 Travelling time to and from their 'home base' to the office is classed as working hours and may be expensed, please refer to the Staff Expenses & Reimbursements Policy.

7.0 Hours of Work

7.1 The employee will work their contractual hours of employment. However, where the role permits the employee will not be subject to any fixed hours, and is free to perform their duties at work times to suit as long as they meet their required outcomes and deadlines and are available as per the job description.

7.2 The employee must keep their manager informed of their working pattern for the week and ensure that they are meeting their job description and fulfilling their statement of terms and conditions of employment.

7.3 The employee must comply with the Working Time Regulation Act 1998.

8.0 Equipment

8.1 All employees that work from home, for any part of their working hours, are expected to provide an appropriate office environment, with a suitable desk and chair in line with the DSE Workstation Assessment.

8.2 It is the Councils' policy to provide and maintain all equipment and materials necessary for you to work from home in line with the following equipment guideline below.

Item	Blended Worker	Homeworker
Laptop	Y	Y
Laptop Stand	DSE Assessment	DSE Assessment
Screen	Y	Y
2nd Screen	Role dependent	Role dependent
Keyboard	Y	Y
Wrist Rest	DSE Assessment	DSE Assessment
Mouse	Y	Y
Foot rest	DSE Assessment	DSE Assessment
Desk	Y - dependent on % of time worked	Y
Office Chair	Y - dependent on % of time worked	Y
Printer	N	Y - dependent on business need
Shredder	N	Y - dependent on business need
Lockable Cabinet	N	Y- dependent on business need
Laptop Rucksack/Bag	Y	Y
Trolley Bag	Role Dependent	Role Dependent

8.3 The Manager will discuss equipment with employees on an individual basis based on their job role, the number of days working from home and the completed DSE Assessment.

8.4 It is the employee’s duty to ensure that proper care is taken of such equipment and materials as they remain the property of the Councils.

8.5 Should the employee not have the right equipment or environment, the manager may request that the employee returns to their main base in line with their contracted hours.

8.6 On termination of employment for any reason, the employee will be required to return all equipment that has been provided to their work base.

8.7 The employee will sign an inventory of items that will be maintained on their file.

9.0 DSE Workstation Assessments

9.1 Line managers have a responsibility to ensure that a health and safety risk assessment is undertaken for each employee in relation to the work-style, practices and location of their work.

9.2 Where employees are visiting clients/sites etc, the line manager and individual must ensure that an appropriate lone working risk assessment is undertaken and appropriate measures implemented in line with the Councils' Lone Working Policy.

9.3 The employee must complete an annual DSE workstation assessment for the home and the office. The employee is responsible for ensuring their workstation is in line with the provided guidelines and that they produce their equipment for annual PAT testing in line with the Councils' processes.

9.4 If the employee's home working environment does not meet the required DSE Workstation assessment standards they may be unable to work safely from home, and they will need to work in the office.

9.5 Employees have a responsibility for implementing any actions identified in order to reduce/mitigate risks to make their work environment safe. The line manager should take reasonable steps to ensure the employee has implemented any actions identified.

9.6 Line managers have a responsibility to ensure that their team members carry out a DSE Workstation assessment, on their home working setup and/or their office base.

9.7 Line managers should review health and safety on a regular basis and it should be discussed frequently during one to one meetings. Where there are concerns, appropriate advice should be sought. This may include employees being assessed by a trained workstation assessor to outline specific equipment needed (e.g. special computer mouse, or a specific type of chair).

9.8 For any accidents that occur in the workplace (which includes the home or any temporary workplace if the accident is work related), the employee should report this to their manager who will complete an accident book report as soon as reasonably practicable and in any case by the end of the current working day. In these circumstances, the line manager should inform the Safety and Resilience team immediately and (if this was not done at the time of the injury) complete an Incident Report Form based on the information given.

10.0 Security and Confidentiality

10.1 ICT policies apply to all employees, wherever they may be working. Employees are expected to maintain the same standards of security of information, system security and security of equipment regardless of their location of work. This includes the Councils' policies on the Data Protection Act , GDPR and the Freedom of Information Act.

10.2 Employees who transport equipment (e.g. laptops, mobile phones) should not, as far as practicable, leave this unattended in vehicles.

10.3 The employee must not allow members of their household or third parties to access or use any Councils equipment.

10.4 Employees who work from home are responsible for keeping all documents and information associated with the Councils secure and confidential at all times. This includes destroying confidential documents appropriately.

10.5 Employee's should not print documents off at home.

10.6 An employee should take the appropriate steps when dealing with confidential matters from home. Where possible, they should ensure they are working in a confidential work space and if taking a confidential call they should wear a headset to mitigate any risk of confidential information being overheard.

11.0 Working Environment

11.1 It's important that staff are able to concentrate on their work and maintain their productivity levels, and distractions kept to a minimum, ie. such as ensuring suitable arrangements for children and dependents is in place.

11.2 Should you require to take leave to look after your dependents more information is available in Section 7: Special Paid Leave within the Leave Policy.

12.0 Stationery and Sundries

12.1 The employee will be expected to order their stationery and sundries from their work location as per the normal procedures. The employee is permitted to take this stationery home for use for work purposes.

13.0 Home domestic bills

13.1 The employee will be expected to pay the costs of all their personal domestic bills. Costs towards household bills, such as gas, water and electricity will not be reimbursed.

14.0 Telephone and Internet Access

14.1 The employee will be expected to pay the costs of all personal telephone and internet connections into their home.

14.2 The employee should not use their personal mobile or phone line for business phone calls.

15.0 Insurance and liability

15.1 The employee is responsible for checking that all home and content insurance policies provide adequate cover for the fact they are working from home.

15.2 Employees are covered by the Councils' insurance policy for employer's liability and personal accident in the same way whether they are office based employees or not.

15.3 Equipment supplied to flexible/mobile workers is covered by the Councils' insurance arrangements, providing it is used for work purposes only, and in line with the manufacturer's instructions.

15.4 It is the responsibility of those who work from home to contact their own insurance company, landlord and/or mortgage provider to advise that they will be working from home.

15.5 The Councils will not reimburse any increase in insurance premium.

16.0 Work Deliverables

16.1 The employee will be measured on outcomes and will be monitored by their line manager. Should an employee complete their allocated workload prior to the end of the daily contracted hours, they must request more work.

17.0 Probation Period

17.1 Any employee who is starting a new role with the Councils may be required to attend the office for training purposes for an intensive period of time before shifting to blended working. This will be agreed with the employee prior to commencement in the role and may vary on a role to role basis.

18.0 Staying in touch

18.1 It is important for the employee to stay in contact with their team and manager on a regular basis.

18.2 The Councils will encourage all employees whether in blended working or home working to attend the office with their colleagues regularly for meetings, training or general work purposes.

18.3 Employees working in a blended work pattern, should at the request of their manager attend the workplace at short notice in the case of an emergency or for business continuity reasons. This will be role dependent.

19.0 Performance

19.1 The manager will have regular 1:1 meetings with their team members to ensure performance is to the required standard and is meeting the managers expectations. 1:1s are encouraged to happen in person whenever possible.

19.2 Should the employees' performance be affected in any way, the manager will commence the normal performance management process as detailed in the Performance Support Policy.

19.3 The manager has the right to request that the employee attends the office on a more regular basis during any period of performance management, to enable support and coaching. This may be up to 5 days a week or in line with the employee contractual working pattern.

20.0 Training and Development

20.1 Should an employee require support in their role, they must raise this with their line manager. This could happen as part of the regular 1:1 conversations that a member of staff has with their line manager

21.0 Disciplinary or Grievance

21.1 The Councils' normal disciplinary and grievance procedure will apply. Should you be required to attend a meeting in relation to either of these procedures you will be expected to attend the meeting at a Councils' premises.

22.0 Visits to the employees' home

22.1 Should the Councils have concerns relating to Health and Safety matters they may request an appointment to conduct an assessment at the employees home. Such appointments will be arranged at a mutually convenient time.

23.0 Dispute Resolution

23.1 Should there be a dispute between the employee and the manager, they should ideally try and resolve it between them informally. If this is not possible then this should be escalated in the first instance to the Head of Service for resolution.

23.2 Should the situation not be resolved within the as per 23.1, then HR should be contacted and then the normal grievance procedure must be followed.

24.0 Failure to comply with this policy

24.1 Failure to comply with any of this policy may result in the employee returning to the office full time and/or appropriate performance management/disciplinary processes being applied.

25.0 Policy Implementation & Monitoring

25.1 Responsibility for the implementation, monitoring and development of this policy lies with the Head of Human Resources and CLT.

25.2 Day to day operation of the policy is the responsibility of managers' who will ensure that this policy is adhered to.

Date policy agreed with Unison: 4th August 2021
Date agreed by Joint Staff Committee: 29th September 2021
Date policy formally adopted: 1st November 2021
Date for review: 1 year from formal adoption of policy 31st October 2022

ADUR & WORTHING
COUNCILS

ADUR & WORTHING COUNCILS INFORMATION SECURITY POLICY

Document Control

Author	Technology Platforms Manager
Current Version	7.0
Implementation Status	Approved / Implemented
Approved by	Paul Brewer
Date of Publication	04/04/2022
Distribution	All staff via the intranet
Last Reviewed Date	04/04/2022

Revision History

Revision	Date	Author(s)	Description
0.1	30/03/2021	SP	Initial version
0.2	14/04/2021	SD,GA	Revised following review
0.3	20/04/2021	GA	Revised following feedback from MK
0.4	21/04/2021	GA	Revised following feedback from TIB meeting
0.5	31/12/2021	GA	Revised following feedback from BR and M
0.6	25/01/2022	GA	Revised after review of policies and guidance already in place
0.7	04/04/2022	GA	Revised following further comments from MW

1. Introduction

- All information held by the Councils, in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.
- The Policy applies to all Members and employees of the Councils, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by the Councils but engaged to work with or who have access to Councils information, (e.g., computer maintenance contractors) and in respect of any externally hosted computer systems.
- The Policy applies to all locations from which the Councils systems are accessed (including home use, the Councils Remote Working Policy is included in Annex A). Where there are links to enable non-Council organisations to have access to the Councils information, officers must confirm the security policies they operate meet the Councils security requirements. A copy of any relevant third party security policy should be obtained and retained with the contract or agreement.
- Suitable third-party processing agreements must be in place before any third party is allowed access to personal information for which the Councils are responsible.

2. Policy Compliance

- Heads of Service should ensure all staff are aware of and understand the content of this policy.
- If any user is found to have breached this policy, they could be subject to Adur & Worthing Councils Disciplinary Policy, which is available on the intranet. Serious breaches of this policy could be regarded as gross misconduct.

- This policy should be read in conjunction with the Councils' Data Protection Policy

3. Legal Aspects

- Some aspects of information security are governed by legislation, the most notable UK Acts and European legislation are listed below:
- The Data Protection Act (2018)
- UK General Data Protection Regulation (UK GDPR)
- Copyright, Designs and Patents Act (1988)
- Human Rights Act (1998)
- Freedom of Information Act (2000)
- Computer Misuse Act (1990)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Protection of Freedoms Act 2012
- Regulation of Investigatory Powers Act 2000
- Privacy and Electronic Communications Regulations 2003
- Counter Terrorism and Security Act 2015
- Common law duty of confidentiality

4. Responsibilities

4.1. Manager responsibilities:

- Be aware of information or any equipment which is removed from the Councils offices for the purpose of site visits or home working.
- Ensure staff are aware of and are signed up to the Adur & Worthing Councils Information Security Policy.
- Enforce the Adur & Worthing Councils Information Security Policy when necessary.
- Ensure staff have the appropriate training and knowledge in the use of the equipment.
- Determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status.
- Ensure staff are unable to gain unauthorised access to the Councils IT systems or data.
- Determine the security level of any data held or accessed by staff. Review the security level of the data annually and ensure compliance with the current regulations.
- Implement procedures to minimise the Councils exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas.
- Ensure current documentation is maintained for all critical job functions to maintain business continuity in the event of relevant staff being unavailable.
- Ensure staff access to relevant systems is kept up to date. This should be based on changes in roles or responsibilities, as well as staff leaving or joining.
- Ensure that any third-party organisations or contractors providing services for the Councils have understood and agreed to the following:
    - Adur & Worthing Councils Information Security Policy
    - Non-Disclosure Agreement
- Ensure information held is accurate, up to date, and retained, in line with the Councils retention and disposal policy.
- Ensure relevant staff are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, Data Sharing Agreements to which the Councils are signatories and the PSN Acceptable Usage Policy.

4.2. Staff responsibilities:

- Be aware of and comply with the content of the Information Security Policy.
- Ensure any mandatory IT Security and GDPR training is completed as required.
- Ensure that no breaches of information security result from their actions.
- Report any breach of data or suspected breach of data to their reporting manager.
- Report any breach of personal data or suspected breach of personal data to their reporting manager and the Senior Information Governance Officer, without delay.
- Ensure information that they have access to remains secure. The level of security of data and information will be determined by a manager.
- Ensure they are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments, or other Data Sharing Agreements to which the Councils are a signatories.

5. Information Security – Data Protection By Design

- The UK General Data Protection Regulation (UK GDPR) requires that organisations put in place appropriate technical and organisational principles and safeguard individual rights. This is known as ‘data protection by design and by default’. This means that we have to integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle. The Councils will, therefore, ensure that privacy and data protection, through its Data Protection Policy, is a key consideration in everything they do. As part of this the Councils will:
    - Consider data protection issues as part of the design and implementation of systems, services, products and business practices, using the Data Protection Impact Assessment (DPIA) process to help identify and minimise the data protection risks of a project, before the project commences and at regular intervals throughout the project .
    - Make data protection an essential component of the core functionality of our processing systems and services and utilise the existing resources available on the intranet for Data Protection Impact Assessments.
    - Anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.
    - Only process the personal data that we need for our purpose(s) and that we only use the data for those purposes.
    - Provide training to GDPR Leads to ensure that their Roles and Responsibilities for their respective services are fulfilled.
    - Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:
    - Potential problems are identified at an early stage.
    - Increased awareness of privacy and data protection.
    - Legal obligations are met and data breaches are minimised.
    - Actions are less likely to be privacy intrusive and have a negative impact on individuals.

6. Personal Data Breaches and Information Security Incidents

- The Councils have a duty to ensure that all personal information is processed in compliance with the principles set out in the UK General Data Protection Regulation (UK GDPR). It is ultimately the responsibility of each Director to ensure that their service areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.
- In the event of staff becoming aware of data breach or an information security incident, they are to follow the Councils Personal Data Breach Notification Procedure. Staff must report any breaches or security incidents (suspected or otherwise), by using the Data Breach Reporting Form which will be actioned and risk assessed by the Council’s Data Protection Officer.

7. Access Control

- Staff, Members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.
- Access to applications and systems are established based on identity and appropriate group membership. Any access for users or groups will need to be requested through Ask Digital.
- All application access requests will need to be approved, at a minimum, by the reporting manager or team that administers the application or system.
- Any changes to the access level needed by a team or a team member will need to be authorised by the reporting manager or team that administers the application or system and the Information Security team.
- Any access to 3rd party applications or systems by the Councils staff should be established by federated identity to the Adur & Worthing Identity Platform.
- Any 3rd party access to applications or systems will need to be established by the following methods in the order of preference:
    - Federated identity to the 3rd Parties identity platform
    - Creating a distinct group with the 3rd party members that need access to the application or system. There will be a time limit on this, which will be determined by the administrators.
    - Authenticating against the Adur & Worthing Councils RADIUS platform.
    - Locally stored user credentials. In such cases, the locally stored credentials will be temporary and only be valid for a maximum of 24 hours. A service request will need to be raised and authorised by the administrators for every new request.
- The Identity platform will need to comply with Adur & Worthing password guidance which can be found in Annex B.
- Any identification devices, access cards, keys, passes or any item that establishes identity or credentials used to gain access to systems should be assigned on a need basis. The system or application administrators/owners should maintain the list of users that have access to these items, and their direct reporting manager. Any change to the status of the user should be communicated to the application administrator/owner within 5 working days so that the use of the security items can be re-evaluated.
- In the event that an employee leaves the Councils, all access should be revoked by their last working day. The employee’s user id in the identity platform should be disabled immediately and deleted within 4 weeks of parting.

8. Security of Equipment

- Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.
- Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.
- Laptops or other portable equipment must never be left unattended in cars or taken into vulnerable areas.
- Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off Council property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.
- Staff working from home must ensure appropriate security is in place to protect Councils equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring Councils equipment and information is kept out of sight. The Councils Remote Working Guidance is included in Annex A.
- Councils issued equipment must not be used by non-Councils staff.
- All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the Councils.
- Users will ensure that all sensitive data is either encrypted or password protected.
- Staff and Members who use portable computers belonging to the Councils must use them solely for business purposes otherwise there may be a personal tax or national insurance liability.

9. PCI-DSS Compliance

- The Councils are currently PCI-DSS (Payment Card Industry Data Security Standard) compliant. This is a set of requirements that ensures that all organisations that handle, process, store or transmit credit or debit card information, meet a minimum security standard.
- All changes, improvements, upgrades or projects should ensure that PCI-DSS security standards are taken into consideration and must ensure that the minimum requirements are met.
- The PCI-DSS compliance must undergo annual audit by an external auditor.
- Any member of staff, who has access to any part of the Councils Cash Receipting systems, whereby they are taking payments either in person or over the phone, should only enter card numbers into the relevant payment screens **only**. Under no circumstances should cardholder data such as card numbers be written down, entered or stored in any device or software that has not been approved by the Councils for this purpose.

10. Security and Storage of Information

- All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:
- Paper files stored in lockable cupboards or drawers.
- Laptops and removable storage such as USB hard drives, stored in lockable cupboards or drawers.
- Electronic files password protected or encrypted.
- Restricted access to IT systems.
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must never be left in unattended vehicles
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive or a removable hard drive such as a flash drive or a usb stick. Access to this type of information must always be through the Councils network.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information.

11. Clear Desk Guidance

- Employees are expected to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into locked desk drawers and cupboards as appropriate.
- Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

12. Information Sharing and Distribution

- Any sharing or distribution of sensitive or confidential information must be done using the most secure method available. In Electronic format that would mean using one of the following methods:
    - Cloud Storage: Users may only use official cloud storage solutions to share information with other colleagues or 3rd party vendors. Access to the information must be restricted to user or group identity.
    - Email: Email directed to particular recipient(s) or groups over Transport Layer Security. Any documents attached to the email should be password protected and the password should be sent separately to the recipient(s).

    - SFTP: Secure FTP for larger file transfers. Any use of secure FTP services should ensure there is adequate security set up on the account. The credentials should not be the default credential and the password should comply with the Adur & Worthing Councils Password Policy . The users must ensure that the SFTP service is hosted or approved by Adur & Worthing Councils.
    Unknown or unverified SFTP services hosted on the internet should not be used, as there is no way to ensure that only the intended parties would have access to the data.
    - Physical storage devices: Users may use physical storage devices such as usb disks, or hard drives to share information. This should be considered as the last option, and only used if none of the other options are feasible. Users should ensure that the device is encrypted. The decryption key should be sent to the recipient separately over an encrypted email.
- In the event that information must be shared by post, the information must be sent using a service that can be tracked and that verifies receipt of the items.
- Any information that needs to be printed, should only be printed on Councils owned printers and using the official print solution. Personal or 3rd party equipment should not be used in any circumstances.
- Any information that is printed should be collected immediately and not left unattended.
- Any printer malfunctions that result in the items not being printed, should be cleared off the print queue by the user.
- When disclosing personal or sensitive information to customers, particularly over the phone or in person, the customer's identity must be verified. Service areas dealing with customers on a daily basis should have suitable security questions which must always be used. If in doubt ask for a suitable ID or offer to post the information (to the contact details you have on file).
- In all circumstances, the user must ensure that they are legally allowed to share the information being requested and only share the minimum amount of information necessary.

13. Retention and Disposal of Information

- Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period.
- Please contact the Senior Information Governance Officer for further advice on retention and see the Retention and Disposal Schedules on the Council’s intranet.
- When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the shredder waste bins. Electronic information must be permanently destroyed.
- When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage.

14. IT Security

- All IT infrastructure including switches, routers, firewalls, patch panels, servers, storage or any other IT equipment that cannot be considered as end user devices or mobile equipment such as Wireless Access Points, must be secured in cabinets which can be locked.
- All equipment must be rack mounted to the racks. If equipment cannot be rack mounted they should be housed in rackable shelves which can be locked.
- All cabinets should only be accessed by authorised personnel who administer the equipment in the cabinets as well as on site security.
- Possession of the cabinet keys should be tracked either electronically or by a secure register.
- Cabinets should be locked when not being accessed by authorised individuals.
- All equipment should not use default passwords. Any built in credentials should be amended to comply with the Councils password policy.
- IT security should maintain a risk register, with all the security exceptions in place. The items, their justifications and mitigations should be periodically reviewed, and signed off by the ICT & Digital Services Manager.
- Any interfaces on servers, switches, routers, firewalls or any equipment which is not in use should be administratively disabled.
- All IT infrastructure should be built based on standard configuration.
- All groups of IT infrastructure should have standard versions and security controls.
- Any deviation from standards should be noted in the Risk Register, with justification and mitigation of vulnerabilities.
- Networks should be segregated to ensure separation of critical production environments from the enterprise and from the management network used for system administration. Separation between environments can be established as having some form of control that regulates access between environments. This control can be in the form of user authentication, device authentication or network access. Furthermore, within the production environment, access between systems or applications should be regulated.
    - The Enterprise environment is the default environment where every Councils user connects on to. This environment allows access to services such as the productivity suite, general file shares, applications that are open to all users as well as the internet.
    - The Production environment is where services are hosted. These can be services that are consumed by all the Councils employees, specific groups of employees or publicly hosted services accessed over the internet or any other method. Within the production environment, there should be separation to ensure that there is adequate separation between systems. The separation would ensure that only authorised traffic between systems is allowed and any unexpected or unintended communication between systems is blocked.
    - The management environment is where system administrators can manage and administer all the IT infrastructure. This environment would host the network management systems and jumpstations. Administrators would by default be in the Enterprise environment, and would establish a secure connection to the management environment, from where they can administer all of the IT infrastructure.
    - Access to management systems and subsequent access to IT infrastructure will be assigned to users based on identity. Identity will provide the basis for access as well

    as the level of access. The use of shared credentials will be limited to read only access. Write privileges can only be assigned to individuals based on their roles.
    - Where possible, local accounts should be disabled or have reduced privileges. Exceptions can be made for root credentials, as due their nature, they cannot be removed or made to have reduced privileges. In such cases, the passwords need to be made sufficiently complex (as per password policy), and made available only to managers.
- Any changes to the configuration of infrastructure should be authorised and tracked. The authorisation and tracking of the changes will be through the Councils change management platform.
- Where possible, encrypted protocols are to be used for management and administration
- All infrastructure will have a method to backup and restore configuration.
- IT support teams will maintain a version history of the backups. The minimum level of version history is 30. This would mean that support staff should be able to roll back to up to the 30th previous version of the configuration or setup.
- All configuration backups, where possible, should be encrypted.
- All configuration backups should only be accessible by authorised personnel. Access should be based on user or group identity.
- All infrastructure should have detailed or debug level logging enabled. Logs should be stored in a remote repository such as syslog or a Security Information and Event Management (SIEM) system.
- All management teams should maintain at least 3 months worth of logs.

15. Internet Usage

- The guidelines for internet usage is applicable to each employee of Adur & Worthing Councils, who require computer and Internet access for their work. Utilising the Internet is allowed and supported as long as the purpose of such usage is to meet the goals of the Councils. Each employee must comply with the rules listed in the policies. Breaching the policies could lead to legal measures taken against the employee. One of these measures is the dismissal from employment. Each of the staff members must realise their responsibility in case of damaging the Councils as a result of such violations. Each employee has to read the policy and comply with it. Any clarifications should be raised with a manager.
- Accepted and supported computer and Internet usage:
    - Internet usage is supported as long as it helps in increasing productivity and it is conducted responsibly. This includes the use of Cloud based productivity tools.
    - All the data shared, posted and received via the Councils equipment belongs to the Councils. It should be managed appropriately and according to the legal policies of the Councils.
    - The equipment available for employees at the working place belongs to the Councils, and its management has all the rights to monitor the Internet activity of all workers. The data transmitted, created and received via the Councils’ equipment can be monitored as well.

    - Any website and downloaded content can be monitored by the Councils. They can be banned and blocked by the Councils if considered harmful to productivity and business as a whole.
- Unacceptable ways of using the Internet at the working place:
    - Any communication, including email, SMS and social media post via the Councils' Internet service or on Council equipment that includes any offensive and/or harmful content. Such content includes language and/or imagery that could be considered as harassment or vulgarity.
    - Accessing or distributing harassing, violent, discriminating, hateful or pornographic messages and imagery by the means of Councils equipment.
    - Utilising the Internet and IT equipment at the working place in order to commit any kind of illegal activity, including piracy of music, movies, and other content.
    - Appropriating someone's login information and using it without permission.
    - Illegally downloading, managing or uploading copyrighted content via the Councils IT equipment.
    - Distributing secret Councils information outside the Councils.
    - Posting derogatory information regarding the Councils, its leaders or other employees.
    - Installing inappropriate software that could be harmful to the equipment and network at the working place.
    - Distributing spam emails and posts via the Councils equipment and the Internet.
    - Posting information based on your personal beliefs and presenting it as those shared by the whole Councils.
    - Each employee should consult with their manager or supervisor in the event of not knowing or being unsure about which actions and information are considered unacceptable.
- All the requirements listed above apply to every user of the Councils equipment and network. Any violation of the set rules can result in legal actions taken by the Adur & Worthing Councils against the person violating the policy. Action may be taken under the Councils' Disciplinary Policy.

16. Third Party Access

- No external agency will be given access to any of the Councils networks unless that body has been formally authorised to have access.
- Guidance can be found on the intranet: Data Sharing Agreements and Data Processing Agreements. No external agency will be given access to any of the Councils networks unless that body has been formally authorised to have access.
- External agencies may be required to sign security and confidentiality agreements with the Councils.
- All external agencies processing personal information on the Councils behalf (including via a hosted IT system) will be required to sign a third party processing agreement.
- The Councils will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.
- The Councils will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the

quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

- All third parties and any outsourced operations will be liable to the same level of confidentiality as Councils Staff.

17. Data Back-up

- Data should be held on cloud storage or a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the IT Operations Manager.
- Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.
- All systems administrators should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a usable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is recommended.
- Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The Councils' Retention Schedule must be followed in determining whether data should be archived.
- Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.
- To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.
- Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.
- If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

18. Software

- All users should ensure that only authorised software is in use on their end user devices.
- Where the Councils recognise the need for specific specialised PC products, such products should be authorised by Digital.
- Software packages must comply with and not compromise the Councils security standards.
- Software packages must integrate with the Councils identity platform.
- The Councils seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to Digital.

- Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact Digital for anti-virus advice.

19. Documentation

- All systems should be adequately documented and be kept up to date so that it matches the state of the system at all times.
- System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.
- Distribution of system documentation should be formally authorised by the system administrator. System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.
- Manual data covered by the Gov Connect (GCSX) must not be removed from the Councils offices in accordance with the agreement.

20. ANNEX A - Remote Working

PURPOSE

The purpose of the Remote Working Guidelines is to describe the security requirements for staff remote access connections to internal IT resources.

MS Direct Access provides secure remote access and enhanced management for Windows laptops managed by Digital.

Users are defined as members of staff, consultants or contractors accessing corporate or business systems and using AWC provided equipment.

POLICY

User Responsibilities

1 Access Rights And Privileges

1.1 Remote users are only permitted to access applications and systems they are approved to access for the purposes of fulfilling obligations to AWC.

Remote users must not permit unauthorised persons, including members of their family, to access AWC's computing or information resources from any computers under their control.

2 Information Management

2.1 Remote users must ensure that the collection, creation, use, dissemination and storage of information relating in any way to AWC's business activities is carried out in accordance with internal Policies, relevant best practice Standards or Guidelines and legislation.

As information is likely to be used offsite, special consideration must be given to maintaining appropriate levels of confidentiality and security in accordance with the classification of the information.

3 Connection Requirements

3.1 After a user has completed a remote session with AWC, they must log out.

Hardware and software installed on remote user's computers must not compromise or interfere with AWC's systems. Remote access may be terminated in the event that normal operations are compromised by a remote user.

4 Audit Trails And System Logs

4.1 AWC reserves the right to monitor and audit the use of remote access Connections. Logs containing details of user activities may be retained.

5 Equipment Use

5.1 Equipment supplied by AWC to users is to be operated and maintained in accordance with corporate Policies. The type of use the equipment is put to must not jeopardise manufacturers' warranties and the equipment should be protected against environmental threats and kept secure just as it would be at AWC's premises.

During a remote session the staff member must remain in control of the PC and in front of it so they can see what is going on.

5.4 Remote management of servers, firewalls and other networked devices is permitted providing strong access controls and additional security mechanisms are used. Management of critical devices may not be facilitated via the internet, but must be achieved through back end connections from the corporate network. Where systems are considered sensitive, a user ID and password may not be sufficiently secure and multi-factor authentication, biometrics or other forms of strong access control may be deemed applicable.

6. Digital Services Responsibilities

Access Requirements

6.1 Authentication mechanisms for remote access must appropriately protect the

information or system being accessed. Remote access to systems requires a multi-tiered approach such as logging into the device and a remote access gateway which provides limited network access or multi-factor authentication.

6.2 Users are restricted to applications
and systems that are essential for them to fulfil work obligations to AWC.

6.3 Should an error occur during the authentication process or the user exceed the number of login attempts, the default setting must be to deny access and the account locked.

7 Encryption

7.1 Remote access links are encrypted by default.

8 Connection Requirements

8.1 When access rights are no longer required, the procedure for termination must be followed. All equipment, hardware, software, etc must be returned and the connection disestablished.

8.2 Systems installed and configured for remote access must not permit any type of real-time in-bound remote access (e.g. telnet, ftp, nfs) unless authorised by the IT Operations Manager. Connections should be achieved through an approved VPN connection or remote access gateway.

8.3 Remote access connections will be installed and configured by authorised IT staff or their agents.

8.4 Where site to site VPN tunnels exist, the tunnel connection will be terminated on the VPN Gateway external logical port and restricted to specific hosts and ports required to support the application. The firewall settings must be forced from the server-side. Users must be restricted to particular systems on the basis of "need to know".

8.5 Network level remote access connections must be terminated through a firewall at both ends of the connection and the appropriate levels of security applied unless the connection is a virtual desktop that prevents processing and storage of information on privately owned or third party equipment. Business to business connections with third parties requires an approved business level firewall.

9 Auditing And Monitoring

9.1 AWC reserves the right to maintain audit logs and monitor remote access connections without notice as and when required to verify systems are working as expected and to ensure compliance with IT Policies.

10 System Support And Maintenance

10.1. System support and maintenance for remote access connections must only be carried out by authorised AWC staff or their designated agents who are technically proficient and understand the implications of specific actions.

11 Training

11.1 Users accessing internal computer systems and information resources by remote access must be educated in the security requirements including how to initiate a access session and gain access to improved systems and how to terminate the when the work is complete.

Correct use of the systems limits the potential for errors and security risks.

21. ANNEX B - Password Guidelines

Passwords are an important aspect of IT security; a poorly chosen password can compromise the security of the Council' critical data and expose the Councils to threats such as unauthorised access, malware and data loss.The below guidelines enforce minimum requirements for both AD and Google accounts to ensure the security of users accounts.

AD Accounts

Password Policy	**Setting**
Enforce password history	24 passwords remembered
Maximum password age	60 days
Minimum password age	1 day
Minimum password length	15 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account lockout policy	**Setting**
Account lockout duration	20 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	20 minutes

Google Workspace Accounts

Password Policy	Setting
Minimum password length	At least 15
Minimum lower case characters	At least 1
Minimum upper case characters	At least 1
Minimum special case characters	At least 1
Minimum numbers	At least 1
Minimum spaces	No restriction
Google password rating	Strong
Password expiry (sso only)	Every 3 months
Require re-logon to change password	Yes
Warn before password expiry (sso only)	7 days
Password recovery	**Setting**
Enable password recovery	Yes
Force password change in cloud manager	Yes
Allow old passwords	No
No. of old passwords	13
2 step verification	**Settings**
Enabled for OU	Yes
Re-challenge user	On each log in
Mandatory enforced from	Thursday 27th October 2016
New user grace period	1 day

22. ANNEX C - Legislation Relevant To Information Security

Human Rights Act (HRA) – Article 8
Everyone has a right to respect for his private and family life, his home and his correspondence.There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others (legitimate aims).

The Article 8 right is a qualified right and permits public authority intervention when this is:
- in accordance with law,
- in the pursuit of a legitimate aim,
- necessary in a democratic society

Common law duty of confidentiality
Information provided in confidence by a third party is protected under the common law duty of confidentiality, subject to the public interest test.
For personal information to have the necessary quality of confidence it:
- Is not in the public domain or readily available from another source
- Has a degree of sensitivity
- Is communicated for a limited purpose and in circumstances where the individual is likely to assume an obligation of confidence, e.g. health practitioner/patient, banker/customer, solicitor/client, social worker/service user, etc.

Data Protection Act 2018 (DPA) & General Data Protection Regulations 2016 (UK GDPR)

The 2018 Act governs and regulates how personal information is used, replacing the 1998 Act of the same name. It incorporates the General Data Protection Regulations 2016. The Act defines six basic rules or principles, which the Council must adhere to. A breach of any of the principles is a breach of the law.

The Act requires the Council to take appropriate technical and organisational measures to protect personal data from unauthorised or unlawful processing and against the accidental loss or destruction of, or damage to, personal information.

Personal information/data is information about a living individual, who can bel identified from that information.

Special category personal data is defined in the Act as:
- racial or ethnic origin
- political opinion
- religious belief
- trade union membership

- physical/mental health
- sexual life
- commission of offences
- proceedings for offences and sentences of Court
- genetic and biometric data
- location data including IP address

There are additional requirements placed upon the data controller for the processing of special category personal data. A data subject is the individual who the personal information is about. A data controller is the organisation/company legally accountable for the personal data that it obtains, uses, holds, etc. Adur District Council and Worthing Borough Council are the Data Controller for the personal data it processes. A data processor is an individual or organisation that processes personal information on behalf of a data controller and under the instruction of the data controller.

Privacy & Electronic Communications Regulations 2003 (PECR)
The Regulations sit alongside the Data Protection Act. They give people more privacy in relation to electronic communications. There are specific rules on:

- marketing calls, emails, texts and faxes
- cookies (and similar technologies)
- keeping communications services secure
- customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings

Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIRs)

The Freedom of Information Act and Environmental Information Regulations give people the right to ask for access to recorded information held by the Council. Some business information held by the Council will be subject to exemption from disclosure under these Acts. The release of such information into the public domain by whatever means will represent a breach of information security.

Protection of Freedoms Act 2012 (POFA)

The Act enhances individuals' privacy rights in some areas. These include CCTV surveillance and processing biometric data.

Computer Misuse Act 1990

The Computer Misuse Act defines a number of criminal offences, relating to hacking, copying of software, introduction of viruses, unauthorised access or modification of computer material and other similar activities. The Act was amended by Part 5 of the Police and Justice Act 2006 to strengthen the legislation around unauthorised access and penalties for helping others to commit computer misuse.

Counter-Terrorism and Security Act 2015

The Act contains a duty on specified public sector bodies, including councils, to have due regard to the need to prevent people from being drawn into terrorism. This is known as the Prevent Duty. The requirements of the Act are embodied in the Prevent Duty guidance. Extremism is defined in the legislation as vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs; or calls for the death of members of UK armed forces, whether in this country or overseas. Radicalisation is defined in the Act as material in support of the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Regulation of Investigatory Powers Act 2000 (RIPA)

RIPA 2000, and The Telecommunications (Lawful Business Practice) Regulations 2000, provides a framework for monitoring activity, data and persons to assist in the detection and prevention of crime in relation to the Council's work. Interception of data or communications must be relevant, necessary and proportionate.

Copyright, Designs and Patent Act 1988

This legislation gives the creators of materials and information rights to control the ways in which their materials may be used. The legislation places restrictions on the copying and use of copyright material including computer software, publications and images and as such unauthorised copies of information, documentation or software may not be made.

Adur & Worthing Equality Impact Assessment (EIA) Template Trial - 2020/21

We want to trial the use of this template when it is appropriate, for example when making significant decisions that may impact disproportionately on certain protected communities. As part of our Good Service Standard we are also seeking to embed these equality impact assessment principles into everyday service planning and delivery. You may therefore only need to complete a template occasionally, but you should always be working to achieve its general principles and intended outcomes.

Our Equality Statement

Adur District and Worthing Borough Councils are committed to increasing inclusion and providing equality of opportunity in all our activities and to ensuring that discrimination does not occur. We will strive for a workforce that reflects the diversity of the local community in order that our services are provided appropriately and the Councils benefits from a wealth of experiences. The Councils will involve the wider community in our decision-making processes and use our influence to progress equality and inclusion issues in the Adur District and Worthing Borough.

To achieve our vision for inclusion and equality we will lead by example, we will listen to our communities and we will seek to work in collaboration with others. As part of this and as set out in Platforms of Our Places; Going Further plan, we will work to establish a platform that will aim to unlock the energy and unleash the power of people in the community to run and improve their own lives and the places they live. We will undertake this work with care, support and respect, recognising the reality of disadvantage and discrimination experinced by many communities.

Equality Impact Assessments (EIAs)

EIAs enable us to consider all the information about a service, policy or strategy from an equalities perspective and then identify actions to support delivery towards our equality objectives and our statutory duties. The EIA process specifically aims to:

- Get the best outcomes for our staff and residents
- Analyse how all our work as councils might impact differently on different groups.
- Help us make good decisions and evidence how we have reached these decisions

EIAs are therefore a practical way in which we can achieve our Good Service standard, where we have pledged to improve our services and make them accessible to everyone. The EIA template we are trialling in 2020/21 is suitable for a number of settings, including policy development, organisation management and service redesign. The template is made up of a series of tables and numbered guidance notes to guide and support you through the approach. We will evaluate the use of the template towards the end of 2021.

Part 1. Equality Impact Assessment (EIA) Template

First, consider whether you need to complete an EIA. Is an EIA needed and is there another way to evidence assessment of impacts. See guidance note **(1)** on the legislative context and guidance note **(2)** on considerations when planning an EIA.

Title of EIA (3)	**Trial - Blended Working Policy**
Team/Department (4)	**All services**
Focus of EIA (5)	**The policy will apply to identified roles across the Council. The roles that it applies to will be identified by the individual HoS and Managers.** **The policy will allow the employee to work in a blended way between home and office. The employee must have an appropriate workstation and environment compliant with DSE guidance.**

2. Update on previous EIA and outcomes of previous actions

If there is no previous EIA, or EIA equivalent or this is an assessment of a new service, then simply write ‘not applicable’.

What actions did you plan last time? (List them from the previous EIA)	**What improved as a result?** What outcomes have these actions achieved?	**What further actions do you need to take?** (add these to the Action plan below)
n/a		

3. Review of information, equality analysis and potential actions

In this section we consider the various protected characteristics groups from the Equality Act 2010 **(6)**

What do you know? (7) Summary of data about service-user / resident / and/or staff feedback.	**What do people tell you? (8)** Summary of service-user / resident / and/or staff feedback	**What does this mean? (9)** Impacts identified from data and feedback (actual and potential)	**What can you do? (10)** ● To advance equality of opportunity, ● To eliminate discrimination, and ● To foster good relations
Age[1]	Younger people may be less likely to have suitable home accommodation for office use (e.g. living with parents or in small flats) Younger people may have lower earning potential and not be able to afford suitable equipment to be a home worker. Older age group may not enjoy the isolation of	● Data Analysis completed of job roles **not able** to work from home (see attached appendix 1). ***Younger workforce not impacted by this change*** according to data ● Data Analysis completed of those people **not wanting** to work from home (see attached appendix 1) Only 6% of staff want	● Complete DSE assessments to see how many people 'cannot' work from home due to known suitable environments and review data. ● Equipment being provided for all relevant staff ● Partial equipment provided for those working at home on an 'occasional' basis ● Culture is being created to ensure that team collaboration still happens face to face. We want everyone to come into the office ● Training for managers on managing isolation, ensuring effective team meetings

[1] **Age**: People of all ages

	working from home. May also have more challenges with technology and remote meetings.	no home working. No areas for specific concern within this data.	● Appropriate training for remote workers on remote meetings, scheduling diaries
Disability[2]	All work environments, whether home, office or other need to be safe, both for people with existing health conditions and prevent ill-health being exacerbated due to poor posture etc. Need to ensure that seating and desks are suitable for team members with musculo-skeletal issues and allow for bespoke furniture (desk and chair). Arriving at work and moving chairs around may not be feasible	● Data analysis shows that there are 12 employee with disabilities known to the council ● 2 Badge holders within the council ● Consideration should be given to 'set desk areas' for those with disability specifically if they are in the office the majority of their working week.	● Review prioritisation and implementation of recommendations from accessibility study (first site visit 02.06.21). ● Survey underway (April 2021) to identify specific needs for each member of staff (to be completed by managers) ● Roll out DSE self assessment process for office and home working, to be reviewed with line managers at 1-1s ● Where required seek advice from the Councils' Health & Safety team or Occupational Health ● Ensure that office layout designs are flexible to allow for additional space where required to suit ● individual assessed needs - **Accessibility Assessment being commissioned**.

[2] **Disability**: A person is disabled if they have a physical or mental impairment which has a substantial and long-term adverse effect on their ability to carry out normal day-to-day activities. The definition includes: sensory impairments, impairments with fluctuating or recurring effects, progressive, organ specific, developmental, learning difficulties, mental health conditions and mental illnesses, produced by injury to the body or brain. Persons with cancer, multiple sclerosis or HIV infection are all now deemed to be disabled persons from the point of diagnosis.

	The flexibility of being able to work from home or other locations will reduce travelling needs. The home environment is more likely to be already adapted for the individual staff member’s particular needs, although not necessarily in terms of their work stations if they have not worked from home previously. The minimum office space standards may not be sufficient for wheelchair users or people who are visually impaired who may need more than the standard minimum. Individual staff may have specific needs which make the new way of working problematic for them (eg: people on the Autistic Spectrum who may have additional sensitivity to noise, or		

	people with mental health conditions affecting their attitudes to consistency or cleanliness).		
Race/Ethnicity	Some ethinc groups live in large family units which may reduce the space to enable them to work from home effectively	● Only 31 employees do not wish to work from home. Currently no data to identify ethnicity impact but based on high numbers of those able to work from home. No concern in this area.	● Data analysis following DSE Assessment to see 'who cannot' work from home.
Gender reassignment[3]	Consideration should be given to ensuring cross functional team training. Teams may be separated when in the office, as may no longer be in 'teams' as worked previously.	● Data not available	● Build into training cross functional training, expecting difference

[3] **Gender Reassignment:** In the Act a transgender person is someone who proposes to, starts or has completed a process to change his or her gender. A person does not need to be under medical supervision to be protected

Pregnancy and maternity[4]	The introduction of greater flexible working opportunities will give women who are pregnant more flexibility to work around medical appointments and potentially be able to work around any issues (i.e. morning sickness etc). Staff on maternity or paternity leave may feel left out of the process, or less well-informed about changes and plans.	● TBC	● New and expectant mother risk assessments that are carried out should ensure they reflect the relocation and changed working arrangements from the end of July and assess whether this raises any additional issues. ● Managers must ensure that they keep staff on leave as well-informed as staff at work, using an agreed method of communication and arranging 'keep in touch' days (or similar) where appropriate.
Religion or belief[5]	Flexible working will allow greater flexibility for religious observance.	● Data not available	● Identification of staff within faith groups most likely to need this service. ● Identify the criteria required for suitable quiet rooms and make space available and publicise as appropriate

[4] **Pregnancy and Maternity:** Protection is during pregnancy and any statutory maternity leave to which the woman is entitled.

[5] **Religion and Belief:** Religion includes any religion with a clear structure and belief system. Belief means any religious or philosophical belief. The Act also covers lack of religion or belief.

Sex/Gender[6]	Higher proportion of part-time staff are female and blended working may not be feasible if living in smaller accommodation (see Lone Parent)	● Data analysis completed see appendix 1. ● No concern - higher number of male full time employees impacted for not working from home. ● Only 18 Female part time employee impacted for not working from home due to their roles servicing the community	● Continue to monitor in normal Management Information reporting ● Reassess when DSE Assessments have been completed
Sexual orientation[7]	No impact identified	n/a	n/a
Marriage and civil partnership[8]	No impact identified	n/a	n/a

[6] **Sex/Gender:** Both men and women are covered under the Act.

[7] **Sexual Orientation:** The Act protects bisexual, gay, heterosexual and lesbian people

[8] **Marriage and Civil Partnership:** Only in relation to due regard to the need to eliminate discrimination.

Community Cohesion[9]	No impact identified	n/a	n/a
Other relevant groups[10]	*See below*		
Carer/Parental responsibilities	Home and flexible working may be beneficial for child care, carer and family commitments: flexible hours will be helpful for school runs and other appointments difficult to arrange outside of traditional working hours. Home environment should be free from unreasonable distractions when someone is working, meaning carers may not	● No data available on the number of employees with carer or parental duties.	● Training to be provided to managers on how to manage these situations to ensure fairness is applied.

[9] **Community Cohesion:** What must happen in all communities to enable different groups of people to get on well together.

[10] **Other relevant groups:** eg: Carers, people experiencing domestic and/or sexual violence, substance misusers, homeless people, looked after children, ex-armed forces personnel, people on the Autistic spectrum.

	be able to fulfil their work and caring/childcare responsibilities. Permitting children to be at home whilst working when over the last 12 months has been allowed, it is now deemed unfair to change rules.		
Home Workers	● Home working may increase feelings of isolation and / or increase the difficulties of "switching off" from work thereby having a negative effect on work/life balance. ● Some posts may be unsuitable for home working even if this is the staff member's preferred option. ● There is likely to be a pay disparity, with lower grade roles less likely to be suitable for home working	No known incidents of this at this time	● Appropriate training Revisit/communicate expectations about no emails after hours/similar ● Continue to monitor through management 1:1 and HR feedback based on sickness absence reporting

	compared to higher paid roles.		
Domestic abuse	- Employees who are in domestic abuse relationships may be at greater risk working from home.	- No identified cases of this known to the council at this time	- Home working will not be mandatory and all employees will be able to work in the office. - Publicise the e-learning available that shows how to spot possible signs of abuse in a home working environment. Amend it to train managers in how to have appropriate conversations with staff. - Signposting information on the staff intranet - HR to monitor through sickness absence reporting - Domestic Abuse policy

4. List the data, information and/or community feedback that informed your EIA

Title (of data, research or engagement)	**Date**	**Gaps in data**	**Actions to fill these gaps: who else do you need to engage with?** (add these to the Action Plan below, with a timeframe)
Staff Survey - 70% of staff who answered survey wanted Blended working	June 2020 Jan 2021	Equalities data missing	Staff need to complete their equality data on Connect

Data Collection from Managers dated June 2021 - 70% of staff want blended working	May 2021	Ethnicity, Location, Hours of work	Add to future reports
Central HR Database report	End of May 2021	Ethnicity	Add equality data

5. Prioritised Action Plan

The Equality Duty is an ongoing duty which means policies must be kept under review. The actions identified below should be incorporated into service or business plans and monitored to ensure they achieve the outcomes identified.

Impact identified and group(s) affected	Action planned	Expected outcome	Measure of success	Timeframe

EIA sign-off:

For the EIA to be final an email must be sent from the relevant people agreeing it or this section must be signed.

Staff member competing Equality Impact Assessment: **Rebecca Mossman-Beckett**	**Date:** **5/6/2021**
Head of Service: **Heidi Christmas**	**Date:** **10/6/2021**
Equality Lead: **Amy Newnham**	**Date:** **14/06/2021**

EIA Guidance Notes

If this is your first EIA, take some time to read through the notes. If you have any questions please email: equalitieschampions@adur-worthing.gov.uk

1. Our duties in the Equality Act 2010

As a public sector organisation, we have a legal duty (under the Equality Act 2010) to show that we have identified and considered the impact and potential impact of our activities on all people with ‘protected characteristics’ (age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marriage and civil partnership). This applies to policies, services (including commissioned services), and our employees. The level of detail of this consideration will depend on what you are assessing, who it might affect, those groups’ vulnerability, and how serious any potential impacts might be. We use this EIA template to complete this process and evidence our consideration. The following are the duties in the Act that we must give ‘due regard’ (pay conscious attention):

- **Avoid, reduce or minimise negative impact** (if you identify unlawful discrimination, including victimisation and harassment, you must stop the action and take advice immediately).
- **Promote equality of opportunity**. This means the need to:
  - ➔ Remove or minimise disadvantages suffered by equality groups
  - ➔ Take steps to meet the needs of equality groups
  - ➔ Encourage equality groups to participate in public life or any other activity where participation is disproportionately low
  - ➔ Consider if there is a need to treat some people differently, including more favourable treatment where necessary
- **Foster good relations between people who share a protected characteristic and those who do not**. This means:
  - ➔ Tackle prejudice
  - ➔ Promote understanding

In addition the following principles, drawn from case law, explain when and how the above duty should be applied:

➔ **Knowledge:** In working for the councils and reviewing its activities staff must be aware of equalities duties and apply them appropriately to this work.

➔ **Timeliness:** The duty applies at the time of considering policy options and/or before a final decision is taken – not afterwards.

➔ **Real Consideration:** The duty must be an integral part of our decision-making and able therefore to influence the process.

➔ **Sufficient Information:** You must assess what information you have and what is needed to give proper consideration.

➔ **No delegation:** The councils are responsible for ensuring that any contracted services which provide services on our behalf can comply with the duty, are required in contracts to comply with it, and do comply in practice. It is a duty that cannot be delegated.

➔ **Review:** The equality duty is a continuing duty. It applies when a policy is developed/agreed, and when it is implemented/reviewed.

➔ **Proper Record Keeping:** To show that we have fulfilled our duties we must keep records of the process and the impacts identified. Properly used, an EIA can form a key part of this requirement.

2. Do you need to undertake an EIA?

An EIA may or maynot be necessary or appropriate:

➔ Is the policy, decision or service likely to be relevant to any people because of their protected characteristics?
➔ How many people is it likely to affect?
➔ How significant are its impacts?
➔ Does it relate to an area where there are known inequalities?
➔ How vulnerable are the people (potentially) affected?

If there are potential impacts on people but you decide not to complete an EIA it is important to document why.

When might you generally complete an EIA:

- ➔ When planning or developing a new service, policy or strategy
- ➔ When reviewing an existing service, policy or strategy
- ➔ When ending or substantially changing a service, policy or strategy
- ➔ When there is an important change in the service, policy or strategy, or in the borough or district (eg: a change in population), or at a national level (eg: a change of legislation)

<u>The EIA does not have to be on this template, but must be documented. Wherever possible, build the EIA approach into your usual planning/review processes</u>. When planning your EIAs remember it should be proportionate to:

- ➔ The size of the service or scope of the policy/strategy
- ➔ The resources involved
- ➔ The numbers of people affected
- ➔ The size of the likely impact
- ➔ The vulnerability of the people affected

The greater the potential adverse impact of the proposed policy on a protected group (e.g. disabled people), the more vulnerable the group in the context being considered, the more thorough and demanding the process is required.

3. Title of EIA: This should clearly explain what service / policy / strategy / change you are assessing **4.**

Team/Department: Main team responsible for the policy, practice, service or function being assessed

5. Focus of EIA: A member of the public should have a good understanding of the policy or service and any proposals after reading this section. Please use plain English and write any acronyms in full first time - eg: ‘Equality Impact Assessment (EIA

6. Protected characteristics groups from the Equality Act 2010:

- **Age**: People of all ages
- **Disability**: A person is disabled if they have a physical or mental impairment which has a substantial and long-term adverse effect on their ability to carry out normal day-to-day activities. The definition includes: sensory impairments, impairments with fluctuating or recurring effects, progressive, organ specific, developmental, learning difficulties, mental health conditions and mental illnesses, produced by injury to the body or brain. Persons with cancer, multiple sclerosis or HIV infection are all now deemed to be disabled persons from the point of diagnosis.
- **Gender Reassignment:** In the Act a transgender person is someone who proposes to, starts or has completed a process to change his or her gender. A person does not need to be under medical supervision to be protected.
- **Pregnancy and Maternity:** Protection is during pregnancy and any statutory maternity leave to which the woman is entitled.
- **Race/Ethnicity:** This includes ethnic or national origins, colour or nationality, and includes refugees and migrants, and Gypsies and Travellers. Refugees and migrants means people whose intention is to stay in the UK for at least twelve months (excluding visitors, short term students or tourists). This definition includes asylum seekers; voluntary and involuntary migrants; people who are undocumented; and the children of migrants, even if they were born in the UK.
- **Religion and Belief:** Religion includes any religion with a clear structure and belief system. Belief means any religious or philosophical belief. The Act also covers lack of religion or belief.
- **Sex/Gender:** Both men and women are covered under the Act.
- **Sexual Orientation:** The Act protects bisexual, gay, heterosexual and lesbian people
- **Marriage and Civil Partnership:** Only in relation to due regard to the need to eliminate discrimination.
- **Community Cohesion:** What must happen in all communities to enable different groups of people to get on well together.
- **Other relevant groups:** eg: Carers, people experiencing domestic and/or sexual violence, substance misusers, homeless people, looked after children, ex-armed forces personnel, people on the Autistic spectrum etc
- **Cumulative Impact:** This is an impact that appears when you consider services or activities together. A change or activity in one area may create an impact somewhere else

7. What do you know (data and Information): Make sure you have enough data and information to inform your EIA.

- ➔ What data, relevant to the impact on protected groups of the policy/decision/service, is available? Consider local sources of data (eg: the JSNA, Local Insight) and national sources where they are relevant.
- ➔ What further evidence is needed and how can you get it? (e.g. further research or engagement with the affected groups).
- ➔ What do you already know about needs, access and outcomes? Focus on each of the protected characteristics in turn. Eg: who uses the service? Who doesn't and why? Are there differences in outcomes? Why?
- ➔ Have there been any important demographic changes or trends locally? What might they mean for the service or function?
- ➔ Does data/monitoring show that any policies or practices create particular problems or difficulties for any groups?
- ➔ Do any equality objectives already exist? What is current performance like against them?
- ➔ Is the service having a positive or negative effect on particular people in the community, or particular groups or communities?

8. What do people tell you (engagement):

You must seek to engage appropriately with those likely to be affected:

- ➔ What do people tell you about the services?
- ➔ Are there patterns or differences in what people from different groups tell you?
- ➔ What information or data will you need from communities?
- ➔ How should people be consulted? Consider:
  - ◆ consulting when proposals are still at a formative stage;
  - ◆ explain what is proposed and why, to allow intelligent consideration and response;
  - ◆ allow enough time for consultation;
  - ◆ make sure what people tell you is properly considered in the final decision.
- ➔ Try to consult in ways that ensure all perspectives can be considered.
- ➔ Identify any gaps in who has been consulted and identify ways to address this.

9. What does this information and feedback mean?

Your EIA should seek to understand the actual and potential impacts.

➔ The equality duty does not stop decisions or changes, but means we must conscientiously and deliberately confront the anticipated impacts on people.

➔ Be realistic: don't exaggerate speculative risks and negative impacts.

➔ Be detailed and specific so decision-makers have a concrete sense of potential effects. Instead of "the policy is likely to disadvantage older women", say if you can, how many or what percentage are likely to be affected, how, and to what extent.Questions to ask when assessing impacts depend on the context. Examples:

◆ Are one or more protected groups affected differently and/or disadvantaged? How, and to what extent? ◆ Is there evidence of higher/lower uptake among different groups? Which, and to what extent?

◆ If there are likely to be different impacts on different groups, is that consistent with the overall objective?

◆ If there is negative differential impact, how can you minimise that while taking into account your overall aims

◆ Do the effects amount to unlawful discrimination? If so the plan must be modified.

◆ Does the proposal advance equality of opportunity and/or foster good relations? If not, could it?

10. What can you do?

Consider all three aims of the Act: removing barriers, and also identifying positive actions we can take.

➔ Where you have identified impacts you must state what actions will be taken to remove, reduce or avoid any negative impacts <u>and</u> maximise any positive impacts or advance equality of opportunity.

➔ Be specific and detailed and explain how far these actions are expected to improve the negative impacts. ➔ If mitigating measures are contemplated, explain clearly what the measures are, and the extent to which they can be expected to reduce / remove the adverse effects identified.

11. Assessment of overall impacts and any further recommendations

➔ Make a frank and realistic assessment of the overall extent to which the negative impacts can be reduced or avoided by the mitigating measures. Explain what positive impacts will result from the actions and how you can make the most of these.

➔ Countervailing considerations: These may include the reasons behind the formulation of the policy, the benefits it is expected to deliver, budget reductions, the need to avert a graver crisis by introducing a policy now and not later, and so on. The weight of these factors in favour of implementing the policy must then be measured against the weight of any evidence as to the potential negative equality impacts of the policy.

➔ Are there any further recommendations? Is further engagement needed? Is more research or monitoring needed? Does there need to be a change in the proposal itself?