Data Protection Policy

Policy Details	
Policy Owner	Executive Director Information Systems & Funding
Date produced	May 2021
Approved by	USP College Corporation, Policies & Procedures Committee
Date reviewed	May2026
Date Approved	May 2026
To be reviewed	May 2027
Publication	MyUSP, USP College Website

1. Statement of Intent

1.1 Individuals whose information is processed by USP College (the college) can be assured that the College intends to fulfill all its Data Protection obligations. This policy applies to personal data processed in accordance with applicable data protection legislation. For the purposes of this policy, "data protection legislation" means the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other applicable legislation and regulatory requirements relating to the processing of personal data, as amended from time to time. Where relevant, this includes guidance and codes of practice issued by the Information Commissioner's Office (ICO)

2. Introduction and Purpose

2.1 The college needs to keep certain information about its employees, students and other users to monitor performance, achievements, health and safety and other legal responsibilities. It also needs to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

3. Statutory Framework

3.1 The college must comply with the Data Protection principles, which are set out in the Data Protection Act (2018) (DPA) and the General Data Protection Regulations (GDPR).

In summary these state that personal data shall:

a. be processed lawfully, fairly and in a transparent manner in relation to individuals.

b. be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes.

c. be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d. be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e. be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and

f. be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2 The college and all staff or others who process or use any personal information must ensure that they always follow these principles. To ensure that this happens, the college has developed this Data Protection Policy.

3.3 The college must also comply with Rehabilitation of Offenders Act 1974, Children Act 1989 and other legislation relating to Further and Higher Education delivery.

4. Related Policies and Procedures

a. Freedom of Information Policy
b. Acceptable Use and Online Safety Policy
c. Compliments and Complaints
d. Safer Recruitment Policy

5. Relevant Legislation

a. Data Protection Act 2018
b. UK General Data Protection Regulation
c. Rehabilitation of Offenders Act 1974
d. Children Act 1989
e. Keeping Children Safe in Education

6. The Designated Data Controller

6.1 The college as a body corporate is the Data Controller under the Act, and the college Corporation is therefore ultimately responsible for implementation. However, the designated data controller will be responsible for:

a. Maintaining the college's registration with the Information Commissioner's Office.

b. Providing advice, guidance and direction on data protection issues within the college.

6.2 The college has a designated Data Protection Officer who is the named person in the notification to the Information Commissioner. This is the Executive Director Information Systems and Funding. The Head of IT is designated as the Deputy Data Protection Officer. All correspondence related to data protection should be addressed to dataprotection@uspcollege.ac.uk

7. Extent of the Policy

7.1 The Data Protection Policy covers all computerised and manual data processing relating to identifiable living individuals. It not only includes information about individuals, but also options and intentions towards an individual. It therefore includes, for example, personnel records about staff, student records, and emails relating to identifiable individuals, curriculum team meeting minutes, student and staff references.

8. Status of the Policy

8.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the college from time to time. Any failures to follow the policy may therefore result in disciplinary proceedings.

7.2 Any member of staff or student, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated data protection officer initially. If the matter is not resolved it should be raised as a formal grievance.

9. Rights to Access Information

9.1 Staff, students and other users of the college have the right to access any personal data that is being kept about them, whether electronically or in structured paper files.. This is known as a Subject Access Request (SAR) under the UK General Data Protection Regulation (UK GDPR).

9.2 Subject Access Requests must be made in writing, either via email or letter. Requests should provide enough detail to allow the College to locate the relevant information. Proof of identity may be required before any data is released. Requests can also be sent directly to the College's Data Protection Officer via: dataprotection@uspcollege.ac.uk

9.3 The college will respond to valid Subject Access Requests as quickly as possible and within one calendar month of receipt. In cases where requests are complex or numerous, the college may extend the response period by up to a further two months. If this is the case, the individual will be notified within the initial one-month period, along with reasons for the delay. Response periods can also be paused while the college validates identification, and the individual will be informed in writing any adjustments to the response deadline.

9.4 In accordance with data protection legislation, the college may apply a reasonable fee for requests that are deemed manifestly unfounded, excessive, or repetitive. Any such fee will be communicated clearly before processing begins.

9.5 Under GDPR regulations individuals also have the right to:

- Request correction of inaccurate or incomplete data
- Withdraw consent where data is being processed under the legal basis of consent
- Request data portability, allowing personal data to be provided in a structured, commonly used, and machine-readable format
- Object to processing and request the restriction of certain types of data processing
- Request erasure of personal data where it is no longer necessary for the purpose it was collected (right to be forgotten)

Some of these rights may be limited by legal or statutory obligations. For example, certain data must be retained for audit, safeguarding, or regulatory purposes, and cannot be erased immediately. Information about retention periods is available in the College's Data Retention Policy. For further information or guidance on exercising your rights under data protection law, please contact the College's Data Protection Officer at: dataprotection@uspcollege.ac.uk

10. Consent

10.1 In many cases, the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions in accordance with the Rehabilitation of Offenders Act 1974 and information about disabilities

10.2 Some jobs or courses will bring applicants into contact with children, including young people between the ages of 16 and 18 and vulnerable adults. The college has a duty under the Keeping Children Safe in Education and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The college also has a duty of care to all staff and students and must therefore make sure that employees and those who use the college facilities do not pose a threat or danger to others.

10.3 Therefore, all prospective staff and students will be made aware of how their data will be processed at the point of application. This consent forms part of the Privacy Statement on the college websites and paper forms.

10.4 The Government and statutory organisations are exempt from the DPA and GDPR regulations, and on receiving a valid "legal exemption certificate" the college will release the requested information to the relevant authorities.

11. Data Sharing

11.1 As a student or staff member of the college, it may be necessary to share your personal data with authorised third parties to fulfil contractual, statutory, or regulatory obligations. This includes, but is not limited to:

- His Majesty's Revenue and Customs (HMRC)
- Department of Education (DfE)
- Office for Students (OFS)
- Student Loan Company (SLC)
- Local Authorities.
- Awarding organisations/exam bodies
- External Auditors

11.2 You will be informed through the college's Privacy Notices about what data is collected, the reasons for processing and the third parties involved. Where consent is required, this will be obtained explicitly. However, the college may not be able to progress with your offer of employment/education without this. In cases where the College has a **legal obligation** or is acting in the **public interest**, certain data may be shared **without your consent**.

11.3 The college ensures that all third-party organisations it shares data with have appropriate data protection and security arrangements in place.

11.4 The college does not routinely transfer personal data outside of the UK or EEA. Where international data transfers are necessary, appropriate safeguards will be implemented in line with UK GDPR requirements.

11.5 The college is committed to a transparent and ethical approach to data sharing, ensuring that data subjects' rights and freedoms are always respected.

11.6 There is no right to references under current legislation; these may be provided by the college with explicit consent from the individual but will be limited to the data held within the relevant retention periods.

12. Special Categories of Personal Data

12.1 Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin

- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

12.2 In most cases where we process special categories of personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

12.3 The processing of special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

13. Retention of Data

13.1 The college will keep some forms of information for longer than others in accordance with legal or statutory obligations.

13.2 Appendix 1 indicates the length of time that records will be retained. This information is in line as set out within the Joint Information Systems Committee (JISC) guidelines full details of this can be found online.

14. Telephone Recording / CCTV

14.1 The college may record telephone conversations for the purpose of training and development and to protect staff and students.

14.2 The college telephone system has the capability to identify sources of calls both internally and externally to the college.

14.3 The college uses CCTV to help prevent crime and for the welfare, health and safety of employees, students and visitors. CCTV will be in operation throughout the college's premises and images securely stored for 30 calendar days, unless a criminal offense has occurred, then it will be handed to the police.

15. Roles and Responsibilities

15.1 All staff and students are responsible for:

a. Checking any information that they provide to the college in connection with their employment or education is accurate and up to date.

b. Correct any errors in information which they have provided.

c. Provide updated information as required i.e. change of address

The college cannot be held responsible for any such errors unless the staff member or student has informed the college of them.

15.2 If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students' course work, opinions about ability, references to other academic institutions,

or details of personal circumstances), they must comply with the Staff Guidelines in Appendix 2.

15.3 IT staff will ensure the college is appropriately protected from external threats for the network and systems under their control.

16. Role-Based Access and Access Revocation

16.1 The college operates a **Role-Based Access Control (RBAC)** model to ensure that staff have access only to the personal data necessary for them to carry out their job responsibilities. Access to personal data is granted strictly on the principle of **least privilege**, meaning users are given the minimum level of access required for their role.

16.2 Access permissions are determined and reviewed by line managers in consultation with IT and the Data Protection Officer (DPO), based on:

- Job function and responsibilities
- Departmental needs
- The sensitivity of the data involved
- Regulatory or contractual requirements

16.3 All systems and applications containing personal data are protected by appropriate technical controls, including password protection, multi-factor authentication (MFA), and access logging.

16.4 Where a member of staff changes role within the College, their access rights will be reviewed and adjusted accordingly. Human Resources (HR) are responsible for initiating this process in advance of any role change.

16.5 When a staff member leaves the College, all access to systems, email, and data is revoked promptly. This process is initiated through formal HR offboarding procedures and carried out by the IT department, usually within 24 hours of the individual's departure.

16.6 Former staff may not retain or access any College-held personal data after their employment ends. Any portable devices, data storage tools, or physical files containing personal data must be returned or securely destroyed

16.7 The College conducts periodic audits of user access rights to ensure appropriate levels of access are maintained and any anomalies are promptly addressed.

16.8 Failure to follow access control procedures may result in disciplinary action and, where appropriate, be reported as a data breach to the Information Commissioner's Office (ICO) in accordance with the College's Data Breach Policy.

17. Data Security

17.1 Data Protection Impact Assessments (DPIA)

a. The college will carry out data protection impact assessments for any new college product, process or procedure that will impact on the use of student or staff data. See Appendix 3 for format.

b. We always carry out a DPIA if we plan to:

i. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.

ii. Process special category data or criminal offence data on a large scale.

iii. Systematically monitor a publicly accessible place on a large scale.

iv. Use new technologies.

v. Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.

vi. Carry out profiling on a large scale.

vii. Process biometric or genetic data.

viii. Combine, compare or match data from multiple sources.

ix. Process personal data without providing a privacy notice directly to the individual.

x. Process personal data in a way which involves tracking individuals' online or offline location or behaviour.

xi. Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.

xii. Process personal data which could result in a risk of physical harm in the event of a security breach.

17.2 Staff Obligations

a. All staff are responsible for ensuring that:

i. Any personal data held is kept securely, for example in a locked room, locked filing cabinet or locked drawer.

ii. If it is computerised, it is password protected. All passwords shall be regularly changed.

iii. Data stored on disks is removed before disposal.

iv. Papers containing personal information are shredded before disposal or securely disposed of by other means.

v. Databases are closed and workstations securely locked when leaving the computer.

vi. Personal information is not disclosed either orally or in writing either accidentally or otherwise to any unauthorised third party.

vii. No personal details should be sent via email unless as part of an encrypted attachment with passwords sent via separate email.

viii. Staff should ensure that no personal data is transported on mobile devices including USB drives, USB drives should only be used to hold personal data with permission from line managers with relevant encryption software installed.

ix. Laptops and mobile devices used by staff travelling between campuses or for the purpose of working from home must be password protected. It is the responsibility of the staff member to maintain the security of equipment and data at all times. Personal data should not be stored locally on laptops and must be saved on the college network and accessed from there.

x. Any personal details that have to be scanned and shared must be done with consent of the person whose data is being scanned and securely removed from the scanning device and subsequent electronic storage following retention protocols.

xi. No personal details of any individuals should be printed or copied without prior consent from the individual and any copies should be securely disposed of following retention protocols.

xii. Any photographs or video taken of individuals must be stored securely with the explicit consent from the individuals for this storage and use.

xiii. Cloud storage should not be used for storage of any personal data including photographs and videos due to the inability to ensure data storage geographical location with the exception of approved providers, list of approved providers is available from IT Services.

xiv. Training is kept up to date annually as provided by the college.

xv. That this policy is followed at all times.

b. Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases. It may also result in a personal liability for the individual staff member.

17.3 Data Breaches

a. Should a personal data breach be detected it will be immediately notified to the Data Protection Officer who will assess the severity of the breach, assessing the risk to individuals and the action to be taken and the breach recorded. The Data Protection Officer will notify the Information Commissioner's Office of all data breaches where a risk to individual's rights and freedoms has been identified.

b. Staff should immediately notify their line managers and the Executive Director Information Systems and Funding (the Data Protection Officer) OR Head of IT (the Deputy Data Protection Officer). Alongside this, the breach information should be sent to dataprotection@uspcollege.ac.uk flagged as urgent.

c. Students should immediately notify Student Services who will notify the Executive Director Information Systems and Funding (the Data Protection Officer) or Head of IT (the Deputy Data Protection Officer). Alongside this the breach information should be sent to dataprotection@uspcollege.ac.uk flagged as urgent.

18. Monitoring, Review and Evaluation

18.1 The college will review this policy every two years or sooner in order to take account of new statutory regulations and recommendations for improvement.

19. Audit Logging

19.1 The College maintains **audit logs** as a standard practice across key systems that process or store personal data. These logs record user access, system changes, and data transactions to support accountability, security, and compliance with data protection legislation.

19.2 Audit logs are used to:

- Monitor appropriate use of data
- Detect unauthorised access or potential data breaches
- Support investigations into data-related incidents.

19.3 Access to audit logs is restricted to authorised personnel and retained in accordance with the College's Data Retention Policy and IT Security procedures.

20. Communication

20.1 The policy is published on the college Intranet (MyUSP) for members of staff. Its review will be communicated by sending an e-mail to all staff; included in the staff newsletter; at staff briefings and/or at professional development days to provide, when required, training for new employees.

20.2 All students will be directed to read this policy within MyUSP and informed of this during enrolment and induction.

20.3 Under the requirements of the Freedom of Information Act 2000, the policy will be listed in the Publication Scheme and made available to the general public on request.

Appendix 1
Summary Guidelines for Archiving Data

Area	Description	Retention	Reason for Collection/Retention
Human Resources	Successful appointment documentation is part of all employees' HR files	**Termination of appointment + 7 years**	**HMRC Safer Recruitment**
Human Resources	Records documenting staff name, dates and role	**Termination of appointment + 10 years**	**Safer Recruitment**
Human Resources	Records documenting the unsuccessful appointment of members staff.	**6 months**	**Employment Tribunals**
Human Resources	Sickness and health & safety records	**Termination of appointment + 40 years**	**Potential Legal Cases**
Human Resources	Details of DBS and any safeguarding concerns	**Indefinitely**	**Safer Recruitment & Potential Legal Cases**
Financial Resources	Records relating to financial services	**Current financial year + 6 years**	**Audit**
Financial Resources	Records relating to funding received that may be receiving European Social Fund (ESF) match funding	**Current financial year + 12 years**	**ESF Audit**
Student Records	Records relating to students in receipt of funding	**Current financial year + 12 years**	**Audit**
Student Enquiries and applications	Data relating to enquiries and/or application to study at the college	**Current financial year + 6 years**	**Potential follow up and appeals**
Examinations	Student results and achievements records	**Current financial year + 10 years**	**Audit**
Learning support	Details of learning support for students	**Current financial year + 7 years**	**Audit**
Photographs	Photos taken as part of marketing events or curriculum requirements	**Stored until requested to remove by individuals**	**Marketing and branding**
Estates	Documentation relating to lettings and hiring of college assets.	**Current financial year + 1 year**	**Potential Legal Cases**
Estates	Images and video captured via CCTV	**30 days**	**Health and Safety**
Estates	Records relating to health and safety including accident logs	**Current financial year + 40 years**	**Health and Safety legislation**
Sports Centre	Membership records	**Current financial year + 6 years**	**Audit**

Ownership and Management of Archives

This includes keeping an up-to-date list of box numbers and disposal dates within the department, preferably by a document stored on the network drive, and arranging for boxes to destroy soon after the disposal date – at least on an annual basis.

Storage and Labelling
Boxes should be clearly labelled with:

- Contents (and whether contents are confidential)
- Unique Box Number
- Disposal date

Full guidelines for data retention can be found online:
http://bcs.jiscinfonet.ac.uk/fe/download_excel.asp.

Appendix 2
Data Protection Act 2018

Staff Guidelines

- Members of staff will process personal data on a regular basis. The College will ensure that all personal data is processed lawfully, fairly and transparently, and only where a valid legal basis has been. These legal bases may include, but are not limited to, the performance of a task carried out in the public interest, compliance with a legal obligation, the performance of a contract, the protection of vital interests, consent, and, where appropriate, legitimate interests

- Information about an individual's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive and can only be collected and processed with their explicit consent as this is not covered by legal obligations.

- Members of staff have a duty to make sure that they comply with the data protection and GDPR principles, which are set out in the College Data Protection Policy. In particular, staff must ensure that records are:

  - Accurate
  - Up to date
  - Fair
  - Used only for the purpose it was collected for
  - Kept and disposed of safely and in accordance with the College policy

- Individual members of staff are responsible for ensuring that all data they are holding is kept securely and securely removed following the retention guidelines and Data Protection Policy.

- Members of staff must not disclose personal data, unless for normal academic, administrative or pastoral purposes, without authorisation or agreement from the data controller, or in line with HR and the College policy.

- Before processing any personal data, all staff should consider the checklist as set out below.

- The HR, Finance and Sports Centre offices are the only departments that should contain all information relating to employees' personal details. Locally stored information within Curriculum areas and departments must be used solely for purposes of communication and collection of any other type of personal data is prohibited.

Staff Checklist for Recording Data

Do you really need to record the information?	
Is the information 'standard' or is it 'sensitive'? (Information about an individual's physical or mental health, sexual life, political or religious views, trade union membership, ethnicity or race is sensitive information)	
If it is sensitive, do you have the data subject's explicit consent?	
Has the individual or data subject been told why and how this data will be processed?	
Are you authorised to collect/store/process the data?	
If yes, have you checked with the data subject that the data is accurate?	
Are you sure that the data is secure?	
If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?	
Have you notified the Designated Data Protection Officer that you intend to hold the data?	
How long do you need to keep the data for, if longer than the retention period as per the Data Protection Policy the designated Data Protection Officer must be notified.	

Appendix 3
Privacy Impact Assessment Template (PIA)

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Equality and Diversity Statement & Impact Assessment

USP College is committed to equality of opportunity. The aim is to create an environment in which people treat each other with mutual respect, regardless of: age, disability, family responsibility, marital status, race, colour, ethnicity, nationality, religion or belief, gender, gender identity, transgender, sexual orientation, trade union activity or unrelated criminal convictions.

This form should be used by managers and policy owners within their area of responsibility to carry out Equality and Diversity Impact Assessments (EDIAs) in relation to protected characteristics including, but not limited to: Age, Disability, Gender reassignment, Marriage and civil partnership, Pregnancy and maternity, Race, Religion and belief, Sex, Sexual orientation. The word 'policy' is taken to include strategies, policies, procedures and guidance notes; both formal and informal, internal and external.

1. Name of Policy

Data Protection Policy

2. Which of the following groups could be affected by this policy?
(Tick all that apply)

Students	√
Staff	√
Wider Community	√

3. Complaints

Have complaints been received from anyone with one or more protected characteristic about the service provided? If yes then please give details.

N/A

4. The Impact

Four possible impacts should be considered as part of the assessment:

a. **Positive Impact -** Where the policy might have a positive impact on a particular protected characteristic.
b. **None or Little Impact –** Where you think a policy does not disadvantage any of the protected characteristics
c. **Some Impact –** Where a policy might disadvantage any of the protected characteristics groups to some extent. This disadvantage may be also differential in the sense that where the negative impact on one particular group of individuals with protected characteristic is likely to be greater than on another.
d. **Substantial Impact –** Where you think that the policy could have a negative impact on any or all of the protected characteristics. This disadvantage may be also differential in the sense that the negative impact on one particular protected characteristic is likely to be greater than on another.

Thought-provoking questions, which might help come to a decision about the impact of a policy on individuals with protected characteristics:

e. Does policy outcomes and service take up differ between people with different protected characteristics?
f. What key information do we have? Does data or engagement with people with protected characteristics give insights into areas of disadvantage, which relate to the policy area?

g. If the policy is likely to have a negative impact on individuals, sharing particular characteristics what steps can be taken to mitigate these effects?
h. Will the policy deliver practical benefits for certain groups?
i. Does the policy miss opportunities to advance equality of opportunity and foster good understanding/ relationships between groups?
j. Do other policies need to change to make this policy more effective?
k. Is there any elements of the policy that could be unlawful under the Equality Act 2010?

Use the guidance provided above and complete the following table: **(Please Tick √)**

Gender/Age	Positive Impact	No or Little Impact	Some Adverse Impact	Substantial Adverse Impact
Gender		√		
Age		√		
Disability	Positive Impact	No or Little Impact	Some Adverse Impact	Substantial Adverse Impact
Visually Impaired		√		
Hearing impaired		√		
Physical Disability		√		
Specific Learning Difficulties		√		
Global Learning Difficulties		√		
Autistic Spectrum Disorder		√		
Any other disability – Various		√		
Other Factors	Positive Impact	No or Little Impact	Some Adverse Impact	Substantial Adverse Impact
Race		√		
Culture		√		
Religious Belief		√		
Sexual Orientation		√		
Gender Reassignment		√		
Marriage/Civil Partnership		√		

Pregnancy /Maternity /Paternity		√		

Please comment on any areas where some or substantial impact is indicated. Any resulting actions must be added to the below action plan.

5. Is there anything that cannot be changed?

What cannot be changed?	Can this be justified?	If so, how?
Not applicable		
E.g., Disabled people can be treated more favorably under the Disability Discrimination Act 2005. If a policy appears to treat disabled people more favorably than other equality groups, the disadvantage may be justifiable		

Please list the main actions that you plan to take as a result of this assessment in your area of responsibility. (Continue on separate sheets as necessary)

Action Plan: None as this is a statutory policy which requires compliance.