South Derbyshire District Council

Potentially Violent Persons Policy

Human Resources Team

March 2018

Contents

Version Control

Version	Description of version	Effective Date
1.0	Warning Marker Register	
2.0	Potentially Violent Person Register	April 1, 2018

Approvals

Approved by	Date
Health and Safety Committee	25th April 2018
Finance and Management Committee	

Associated Documentation

Description of Documentation	
Lone Worker Policy	

1.0 Introduction

1.1 South Derbyshire District Council ("The Council") is committed to providing customer focussed, value for money services for the Community.

1.2 Unfortunately and in a minority of cases, employees and Elected Members may from time to time come into contact with persons that may demonstrate aggressive, potentially violent or unreasonable behaviour. Furthermore hazardous premises or sites may also pose a risk to their health, safety or welfare.

1.3 It is recognised that employees who work in direct contact with the public either out on site or in the offices and those who undertake lone working both during and outside normal office hours will be the most at risk.

1.4 The Council has a responsibility to protect employees at work from the risks associated with their health and safety. Accordingly, the Council is committed to ensuring that the health, safety and welfare requirements of its employees are fully met and that any risks to them are managed and minimized.

1.5 It is also important to recognise that other types of behaviour from members of the public also present a risk to employees. This includes behaviour related to hate crime and sexual abuse and it is intended that this Policy would also include these types of behaviours to afford the necessary risk management actions for Council employees.

2.0 Purpose and Objectives.

2.1 The purpose of this Policy is to:

- Define what the Council considers to be aggressive, potentially violent or unreasonable behaviour and to ensure fairness and consistency when dealing with such behaviour.
- Provide options that are available to the Council to protect employees from such behaviour.
- Explain the possible consequences such as being placed on the Potentially Violent Persons List ("PVL").
- Ensure that all customers are treated equitably and on an individual basis.
- Set out the Council's procedures and provide guidance on the use of information relating to potentially violent persons.

2.2 The Policy will provide:

- Compliance with statutory legislation and guidance in the protection of employees from the risks of lone working and potentially violent behaviour. (**See section 4 - Legal requirements**).
- So far as reasonably practical, to protect employees from the risks of aggressive and potentially violent persons.
- For the introduction of a corporate system for listing Potentially Violent Persons (or hazardous premises where risks are known and person(s) either not present or identifiable), that all employees can reference, to enable them to eliminate or significantly reduce the risk of harm or injury.
- That the corporate system is made available across all Council services and controlled centrally to ensure appropriate levels of governance and security of the information is maintained at all times.
- For information to be shared across the Council where employees are issued with work tickets or service requests from members of the public and enable electronic and/or

manual documentation to be marked in such a way that it highlights the risk to employees.

- Recognition of the rights of individuals who may appear on the list and to ensure that all necessary steps are complied with in accordance with appropriate legislation governing accessing records and information.
- That appropriate steps are taken to ensure that the corporate system is maintained and updated in a compliant, transparent and timely manner.

3.0 Definitions

3.1 Aggressive behaviour and or violent behaviour can cause physical or emotional harm to others. It may range from verbal abuse to physical abuse. It can also involve harming personal property, facilities or work equipment.

3.2 'Unreasonable behaviour' - Abusive, persistent or vexatious complaints and customers behaviour whether face-to-face, by telephone, social media, or written that may cause staff to feel intimidated, threatened or abused.

3.3 Hate crime - A range of criminal behaviour where the perpetrator is motivated by hostility or demonstrates hostility towards the victim's disability, race, religion, sexual orientation or transgender identity.

3.4 Sexual abuse - Sexual abuse is any sort of non-consensual sexual contact either verbal or physical.

3.5 'Hazardous premises' - The potential to cause physical harm with the consequences to persons receiving an injury, or contracting ill-health or disease.

3.6 The 'Policy' comprises this document and any supporting systems or documentation as referenced in the Policy.

3.7 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person as defined in section 3 of the DPA 2018.

3.8 Data Protection Legislation means the Data Protection Act 2018; the EU Data Protection Directive 95/46/EC; the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016); the Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; the Electronic Communications Data Protection Directive 2002/58/EC; the Privacy and Electronic Communications (EC Directive) Regulations 2003; and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner.

3.9 Data Protection Officer ("DPO") means the role as defined under section 69 of the Data Protection Act 2018

3.10 Data Controller means as defined in the Data Protection Act 2018

3.11 Data Processor means as defined in the Data Protection Act 2018

3.12 DPA means Data Protection Act 2018

4.0 Legal Requirements

4.1 Health and Safety at Work Act 1974 states that; “It shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees.”

4.2 Health and Safety at Work Act 1974 & The Management of Health and Safety Regulations 1999 imposes a duty on employees to take reasonable care for their own safety and that of others and to co-operate with the employer with their safe systems of work.

4.3 The Data Protections Act 2018 regulates the processing of personal data. It gives rights to individuals (data subjects) and places obligations on those who control the processing of personal data (data controllers) who must comply with six principles, which form a framework for the proper handling, collection, processing, retention, security, use and destruction of personal data.

4.4 Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR). The statutory requirement to record and report incidents of work related violence.

5.0 Compliance

5.1 The Data Protection Act 2018 [DPA]. The DPA sets out the data protection responsibilities for organisations. They are based on six principles that form the fundamental conditions which organisations must follow when collecting, processing and managing personal data.

The six principles of the DPA require that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. 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.
5. 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 DPA in order to safeguard the rights and freedoms of individuals.
6. 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.”

5.2 The Council has adopted local arrangements to meet its obligations under the DPA and these are available at www.south-derbys.gov.uk

5.3 Services are expected to comply with the DPA at all times and to develop their own local arrangements as required.

6.0 System Administration and training

6.1 The corporate system will consist of a separate secure database on a shared area of the Council's main network server that will give restricted view only access to authorised employees across all departments throughout the Council. Direct access will only be given to duly nominated and authorised employees and will be subject to regular review, at least once a year.

6.2 Where just cause necessitates an entry onto the database, a marker will be attached to the database to warn an employee of a potential hazard. The marker will identify that a risk is attached to a property, location or person (s).

6.3 The system will be maintained by trained staff and only authorised entries will be included on the system. These trained staff will have full editing and control over the information maintained on the system under the supervision of the Potentially Violent Register Co-coordinator and/or nominated Officer(s) in their absence.

7.0 Operating System

7.1 The Council will operate a corporate system on a database ("the register") with restricted access upon which persons, property or locations considered to be potentially violent or present a risk to employees are recorded by the Potentially Violent Register Co-ordinator.

7.2 This register will replace all individual departmental lists or registers, which are no longer acceptable and have been securely destroyed.

7.3 The use of potentially violent markers on existing files is also governed by the data protection compliance issues set out in this Policy.

8.0 Fair & Lawful Processing

8.1 The DPA principles as noted in section 5, places a number of obligations on the Council in relation to the collection of personal data, which includes:

- Transparency: Tell the subject what data processing will be done.
- Fair: What is processed must match up with how it has been described
- Lawful: Processing must meet the tests described in the DPA

8.2 The Council will rely upon the following condition to meet compliance with the DPA;

- The processing is necessary for the purposes of exercising or performing any right or obligation, which is conferred or imposed by law on the data controller in connection with employment as a result of the duties imposed on employers under health and safety legislation.

8.3 The Council will in determining the decision to place an individual on the PVL will take into consideration whether the individual has a known or suspected:

- Alcohol or drug abuse
- Mental illness/disability
- Serious Illness or disability
- History of violent behaviour/ criminal convictions
- Aggressive behaviour

To comply with the DPA and as soon as the decision is made, the Council will inform the individual that they have been identified as being potentially violent and that they will be included on the Council's PVL. This will:

- Detail the action the Council has taken and the reasons.
- Advising them of their right to appeal.
- Explain what it will mean for the individual's future contact with and service from the Council.
- Set out whether there will are restrictions placed on the individual in terms of contacting the Council.
- Advise on how long any restrictions will remain and the date of any reviews.
- Advice on the length of time the individual will be placed on the PVL and the date of review.
- Explain that the decision will be notified to employees, Elected Members and may include other organisations such as the Police, in accordance with clause 11.8 below.

8.4 Only after the individual is notified of the decision and any Appeal periods have expired will they be added to the corporate register. The individual will be entitled to request further information on why their actions have caused them to be included on the register and to challenge the length of time the details will be held on the register within 14 calendar days of being notified of the decision. All decisions will be confirmed in writing.

8.5 In exceptional circumstances, the Council may decide that informing the individual of being placed on the PVL may create a significant risk of harm or a violent reaction thereby placing employees at significant risk. In this circumstance the individual will not be informed, however the decision maker will record evidence as to why this decision has been taken and will be subject to review.

8.6 The individual will have the right to appeal in writing within 14 calendar days of being informed that they are being placed on the PVL. Once an Appeal has been submitted within the 14 calendar days, the Council will review its decision and communicate the final decision within 28 calendar days of receiving the Appeal.

9.0 Decision to Identify Individual's as Potentially Violent.

9.1 The Council has identified the Strategic Director (Corporate Resources) as the officer with corporate responsibility for the system and for making final decisions about the identification of individuals who are potentially violent. This officer is the Potentially Violent Register Coordinator ('the Coordinator)

9.2 In the absence of the Coordinator all final decisions will be made by the Head of Organisational Development ("HOD") and /or Health & Safety Officer ("HSO")

10.0 Duties of the Potentially Violent Register Coordinator.

10.1 The Coordinator will make decisions as to whether an individual should be:

- Entered on the register based on full consideration of the evidence provided.
- Restricted on the number and duration of contact with employees in a given time period.
- Limited to one method of contact.
- Provide a single named point of contact for all communication. This should be a senior manager within the relevant Department.
- Determine if the information should be shared with other parties such as the Police, contractors and/or Elected Members.

- Complete regular reviews of the data held on the PVL
- Authorise and keep under review those employees who maintain the database and those given 'view only' access.

The Coordinator will ensure that the fair processing provisions of the DPA are complied with.

The Coordinator shall ensure that any physical, sexual, hate crime or racial abuse will be reported to the Police.

10.2 Individuals who are thought to present a real and significant risk should be identified on the register. Consideration will be given to recording an entry on the register where there has been an actual incident of physical violence, harassment or abuse to an employee, Councillor, contractor or agent of the Council which caused that individual to have a genuine fear for his/her safety. In very limited cases, the Coordinator may include an individual in the register on the basis of intelligence, or factual information received from a credible third party e.g. the Police. In such a case, the Coordinator will review the information and determine whether an entry will be made in the register. If so, the entry will be clearly marked "information received from a third party which is based on a statement of fact."

10.3 All decisions will take account of the nature of the incident, the degree of violence used or threatened, and whether or not the incident indicates a credible threat of violence or significant risk of harm to an individual. The information held will be relevant and not excessive in accordance with the principles of the DPA.

10.4 The following background information and mitigating factors will also be considered when deciding whether to include an entry on the system and where necessary details will be included within the entry:

- Nature of the incident.
- Degree of violence used or threatened.
- Level of injury or harm sustained.
- Level of impact to the victim.
- Likelihood that a repeat incident could occur.
- Previous history of violence, abuse, harassment and likelihood of repetition.
- Mitigating factors i.e. personal tragedy or illness.
- Behaviour/conduct of employee involved.
- Credibility of the information and its source.
- Reliability (where appropriate) of identification.
- Corroboration of the incident by other members of staff or other witnesses.

10.5 All decisions are fully documented. An entry will comprise of:

- Name and address of the member of the public concerned
- A brief description of the incident
- The source of the information
- Mitigating/background information
- Date of entry
- Date of review

10.6 Where insufficient information/evidence is provided on the assessment form to enable a decision to be made; the matter will be deferred to enable further information/evidence to be obtained. In certain circumstances, the employee may be interviewed by the Coordinator to ensure sufficient information is provided to enable a decision to be made. In the event that the Coordinator requires further information, which is not forthcoming, no entry will be made on the register.

10.7 All entries are reviewed on a six-monthly basis and names removed from the system if appropriate. When entries are removed, the Coordinator will take appropriate action to ensure that;

- The individual is informed
- All Council services are aware that the person no longer presents a risk
- All record of the entry is securely destroyed in accordance with the requirements of the DPA

10.8 Only those employees and other individuals undertaking work on behalf of the Council with a legitimate reason to be made aware of information held on the system will be given access to it.

11.0 Adding/Altering/Removing Data

11.1 All data to be added to the system or alterations or removal to existing data shall be approved by the Coordinator or in their absence by the Health and Safety Officer or Head of Organisational Development.

11.2 The Coordinator, Health and Safety Officer or Head of Organisational Development shall ensure that the information posted is concise, legal, accurate and appropriate before approval is given.

11.3 The information contained on the system will be reviewed every six months and the Coordinator will approve any necessary alterations and deletions of data.

NOTE: An individual has a legal right of access to receive a copy of the data held about them and a right to compensation if it is inaccurate.

11.4 An individual, premise or location will be registered once the assessment form has been completed and a decision is reached to register by the Coordinator or Health and Safety Officer and/or Head of Organisational Development.

NOTE: Whilst the provisions of the DPA do not apply to premises or locations, the principles of the DPA would still be observed to ensure that data is correctly logged and reviewed.

11.5 If an individual is not registered on the system then no further action will be taken.

11.6 If the decision is taken to register then formal confirmation will be sent out to inform the individual that they are now on the Council's potentially violent person's database – subject to the completion of any Appeal.

11.7 If an individual is then identified as presenting an increased risk or has again been involved with an incident with a Council employee or other persons working on behalf of the Council between the date of the first incident and the date of their removal from the database then the date for removal will be increased by a minimum period of 12 months.

11.8 The Council reserves the right to share this information with other interested parties such as Councillors, Contractors and other agencies where the law requires it. Information may also be shared where the Council has a legal duty to do so and for the prevention and detection of crime. Information will be shared as and when the need arises.

11.9 The Coordinator will meet with the Health and Safety Officer or Head of Organisational Development every six months to review the database and further improvements or amendments to this Policy. The Policy will be reviewed every two years or when there is new or amended legislation that requires the Council to do so.

13.0 Review of Entries

13.1 The DPA requires that information is accurate and where necessary kept up to date and requires that information shall not be kept for longer than is necessary.

13.2 All entries will be reviewed every six months to ensure that they are accurate and up to date and to ensure that people are not identified as being potentially violent when no threat remains, and entries removed where appropriate. Retention of entries will be for a minimum period of six months and will depend on the level or threat of violence in the original incident, the length of time since the incident, the previous and subsequent behaviour of the individual and any mitigating circumstances.

14.0 Nominated Officers

14.1 Each Service will nominate an Officer with responsibility for coordinating matters relating to the PVL. The Nominated Officer, subject to the approval of the Coordinator, shall:

- Coordinate assessment forms within their service which will be forwarded to the Coordinator.
- Ensure that only those employees who are likely to come into contact with a potentially violent person(s), through visits or by meeting in open plan reception areas, or who can otherwise demonstrate a need to know, will have access to information held on the PVL.
- Keep the information from the database secure, controlled and not included on any other system without the formal permission of the Coordinator.
- Adopt and review local procedures in their own service to ensure that employees and third parties working on behalf of the Council are aware of the PVL and that it is checked before service is provided to a member of the public or visit to a property or location is made.
- Check the register on a regular basis and ensure that any changes to the database are properly communicated.
- Ensure that the stated principles of the DPA are observed at all times when undertaken the role.

15.0. Referrals

15.1 Any employee who genuinely considers that an individual should be entered on the register as potentially violent should complete an assessment form. The form should by authorised by the employee's manager and passed to the Nominated Officer within the service unit. The Nominated Officer will pass it to the Coordinator for a decision on whether it will be included on the register in line with this procedure. The employee may be interviewed by the Coordinator if further information is required to enable a decision to be taken as necessary.

15.2 All information should be completed without undue delay and forwarded on to the appropriate persons on the same or next working day where ever possible.

16.0. Training

16.1 Nominated employees will be trained in the proper use of the system, requirements of the DPA and this policy and the procedures that need to be followed. For example, they should

be aware that they have a duty to report incidents, the type of incidents which should be reported, and the officer to whom they should pass this information.

16.2 All employees at the Council are required to attend mandatory training on data security and the requirements of the DPA. In addition, employees, where appropriate, will also be provided with training in avoiding conflict at work and other relevant health and safety training as required.

17.0 Security

17.1 The information on the register will be governed by security measures which prohibit unauthorised access, disclosure, alteration, loss and destruction in accordance with the requirements of the DPA.

17.2 Only those employees who are likely to come into direct contact with a potentially violent individual, through visits or by meeting in open plan reception areas, site visits or who can otherwise demonstrate a need to know, will have access to information about that individual held on the register. The right to access information will be strictly controlled, reviewed and maintained by the Coordinator.

17.3 All records containing an indication that an individual is potentially violent will be retained securely. All necessary steps will be taken to prevent unauthorised access to any manual or electronic information indicating that an individual has been violent. Unlawful disclosure of information is a criminal offence under the DPA.

18.0 Passing the information to other organisations

18.1 In accordance with the DPA - Personal data shall not be transferred to a country or territory outside the European Economic Area ("EEA"), unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. Personal data should not be transferred outside the EEA without authorisation from the Coordinator or the DPO

18.2 In some cases the Council may consider that another organisation that is likely to have contact with an individual considered to be potentially violent should be made aware of this fact.

18.3 In passing on (or disclosing) such information the Council will ensure it is only completed in accordance with the requirements of the DPA. Advice will be south from the Data Protection Officer before any information is released and stated examples in the DPA when this may occur include;

- for the exercise of any functions of a public nature exercised in the public interest by any person

- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment which would otherwise justify the processing of sensitive personal data by the Council. This is because the duties imposed by health and safety legislation on an employer to protect his employees are imposed on that employer only in respect of his employees.

- The processing is in the substantial public interest; is necessary for the purposes of the prevention or detection of any unlawful act; and must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice these purposes.

However, this will only be applied on a case-by-case basis when there is a credible risk that an unlawful act, such as an assault, will occur. The Coordinator should be notified of any proposed disclosure and ensure that it is noted in the register entry. Unlawful disclosure of information is a criminal offence under the Act.

18.7 Whatever the basis of the disclosure being made the Council will inform the individual that their data has been passed on, the stated reason under the DPA that enables data to be shared and to whom.

18.8 It is important that strict compliance with the DPA is observed at all times when data is shared and advice must be sought in advance from the Data Protection Officer.

19.0 Individual rights

19.1 Individuals have the legal right to request access to any information held about them. This will include the fact that an individual may have been recorded as being potentially violent although in line with this Policy, the individual will have been informed of this in advance.

19.2 Individuals who request access to information held will be required to pay a fee and supply proof of identification such as photographic ID, driving licence or passport

19.3 Under the DPA individuals also have the right to require the Council to cease the processing of personal data which is likely to cause them substantial and unwarranted damage or distress. If the individual is not satisfied with the Council's response he/she has the right to make an application to the court and the Council may therefore have to justify the entry on the register. If an entry cannot be justified, is inaccurate or out of date, compensation may be awarded to the individual.

20.0. Data Protection Queries

20.1 The Coordinator should be contacted with regard to any data protection queries in respect of this policy.

20.2 Any matters related to the processing, control, privacy and other matters related to the handling of data should be referred to the Data Protection Officer.

21.0 Review

21.1 This Policy will be reviewed every two years.