canterbury city council

Customer Behaviour and Incident Policy

August 2018

Document Title	Customer Behaviour and Incident Policy
Revision No.	v1.0
Release Date	September 2018
Review Date	August 2021
Document Type	Draft Policy

Purpose

The purpose of this document is to:

- Explain the reasons for considering customer incidents to be included on the Customer Behaviour and Incident Register
- Define and explain what we consider to be a customer incident
- Define and explain all other risks to staff that are to be included on the Customer Behaviour and Incident Register
- Explain the process the Customer Behaviour and Incident Register group will follow so that everyone knows what they can expect
- Define and explain what we consider to be unreasonable customer behaviour
- Define and explain what we consider to be vexatious requests
- Explain the process we will follow when dealing with customers who behave in an unreasonable way so that everyone knows what they can expect
- Explain the process we will follow when dealing with vexatious requests so that everyone knows what they can expect

Introduction

Many council services are delivered by staff on a face to face basis with customers. This may be in its own buildings, other organisations, public places or a customer's home. This contact often requires staff to pass on unwanted news or take enforcement action, for example refusing permission, informing on unsuccessful applications, issuing fixed penalties etc.

Although uncommon, customers (or perhaps someone with them) might become aggressive, abusive, threatening or even violent as a result of the conversation. This type of reaction could also be triggered or exaggerated if the individual is already in a heightened emotional state perhaps due to personal circumstances, illness, medication etc. Predicting when and where this

might happen is impossible. However, access to information on previous incidents together with suitable training and experience in recognising and managing difficult situations ensures visiting officers are better equipped to make an informed decision as to how to provide a service without putting themselves at risk.

The Customer Behaviour and Incident Policy is a corporate process and system (operating within the boundaries of the Data Protection Act), which facilitates the sharing of information on potential risks to staff with all visiting officers. This system is populated by information received from staff either as a result of an incident or a professional concern. Risks identified will include those presented by individuals, but also those posed from dangerous animals, dangerous structures, presence of needles or weapons etc.

The register is one of the lone working tools staff can use. Just because a customer or property doesn't appear on the register it doesn't mean a situation or incident won't occur. All staff should apply their training and other lone working procedures to ensure their safety.

In a minority of cases, people pursue their complaints or requests for information in a way that is unreasonable. In some instances this can have a negative impact on the handling of their complaint or request. It can also have a significant impact on our resources and on our ability to provide services to our other customers.

What is a customer incident, risk to staff or unreasonable/vexatious customer behaviour?

We define a customer incident as:

"Any interaction with a customer which has or could result in, a risk to staff safety, wellbeing or their ability to effectively carry out their duties."

We define a risk to staff as:

"Any hazard created by a situation or environment type which is likely to present a risk to staff safety, wellbeing or ability to effectively carry out their duties."

We define unreasonable customer behaviour as:

"Behaviour which, because of the nature or frequency of a customer's contact with the Council, negatively impacts upon our ability to deal effectively with their or other people's complaints"

We differentiate between persistent customers and unreasonably persistent customers.

Customers making a complaint can be persistent where they feel that we have not dealt with their complaint properly, and are not prepared to leave the matter there. For example, it is not unreasonable for a customer to criticise how their complaint is being handled when our published procedures are not followed.

However, some customers may have justified complaints or requests but may pursue them in inappropriate ways e.g. lengthy phone calls, emails expecting immediate responses, detailed letters or emails every few days. Others may pursue complaints or requests which have no substance, or which have already been considered and dealt with. Their contacts with us may be amicable, but still place very heavy demands on staff.

Situations can escalate, and in a few cases customers can become abusive, offensive, threatening or behave in a way that we may consider to be unacceptable.

In these circumstances, we may have to restrict access to our premises or staff, in order to protect staff from harassment and/or harm.

We define a vexatious request as:

A request that is likely to cause distress, disruption or irritation, without any proper or justified cause.

A vexatious request may include one or two individual requests for information, or may form part of a wider pattern of vexatious behaviour. For example, if there is a wider dispute or it is the latest in a lengthy series of overlapping requests.

We will consider each request for information on its own merits, and will not automatically refuse a request because the individual may have caused problems in the past. We will ensure that we consider whether the request (and not the requester) is vexatious, with our focus being on the request itself.

Where a request is considered to be vexatious we may make the decision not to provide the information requested, referring to relevant guidance from the Information Commission on vexatious requests.

Examples of incidents, risks to be reported and unreasonable/vexatious customer behaviour

The register can only be as effective as the information received, so staff are encouraged to report all incidents or information relating to possible risks to staff safety. Examples of what we may consider for inclusion on the register are shown below.

- Actual physical violence
- Threats of violence.
- Potential physical violence

- Severe verbal aggression or abuse
- Injury from or threat using a weapon
- Injury from or threats using a dangerous animal
- Identification of a dangerous structure
- Injury from or a threat of injury from a motor vehicle
- Injury from hazards identified in a property

This list includes the most common types of incident, however it isn't exhaustive. If there is any doubt as to whether an incident should be reported or how it should be reported please contact the CCC Corporate Health and Safety Manager.

Examples of what we might consider to be unreasonable behaviour are shown below. The list is not exhaustive, nor does one single feature on its own necessarily imply that the person will be considered as being in this category:

- Refusing to specify the grounds of a complaint, despite offers of assistance.
- Changing the basis of the complaint/request as the matter proceeds.
- Denying or changing statements made at an earlier stage.
- Covertly recording meetings and conversations.
- Submitting falsified documents from themselves or others.
- Making excessive demands on the time and resources of staff with lengthy phone calls, emails to numerous council staff, or detailed letters every few days, and expecting immediate responses.
- Refusing to accept the decision; repeatedly arguing points with no new evidence.
- Persistently approaching the council through different routes about the same issue.
- Causing distress to staff.
- Making unjustified complaints about staff who are trying to deal with the issues, and seeking to have them replaced.

Examples of what we might consider to be vexatious requests are shown below. The list is not exhaustive, and for a request to be considered as vexatious it is likely that more than one of the examples is relevant:

- Submission of obsessive requests with very high volume and frequency of correspondence
- Requests for information the requester has already seen, or clear intention to reopen issues that have already been considered
- Where complying with the request would impose significant burden on the council in terms of expense, and negatively impact upon our ability to provide service to others. In this situation we will also consider section 12 (exemption where cost exceeds the appropriate limit) of the Freedom of Information Act.
- Where the requester states that the request is actually meant to cause maximum inconvenience, disruption or annoyance.
- Where the request lacks any serious purpose or value. An apparent lack of value would not usually be enough on its own to make a request vexatious, but may do when considered with other examples.
- Harassing the council. This could include very high volume and frequency of correspondence, or mingling requests with accusations and complaints.

All incidents involving staff and potential risks to staff should be recorded on the corporate Customer Behaviour and Incident Form which is on the internal staff intranet and on completion is automatically sent to the Corporate Health and Safety Manager. This ensures that an initial assessment of the risk is made quickly, the information relating to the member of staff is recorded and any reporting to the Health & Safety Executive is completed.

If the customer is already on the register a new 'Customer Behaviour and Incident Form' should still be completed for each incident so the register entry can be reviewed and additional action taken if necessary.

Considerations before action

We recognise that the decision to classify someone's behaviour as unreasonable, or to classify a request for information as vexatious, could have serious consequences for the individual, including restricting their access to services.

Before deciding to apply any restrictions, we will ensure that:

- The complaint or request for information has been dealt with properly and in line with the relevant procedures and statutory guidelines

and

- We have made every reasonable effort to satisfy the request or resolve the complaint

Where our efforts to resolve matters with the customer have not been successful we may close the case or request. Where appropriate we will advise the customer to contact the Local Government Ombudsman or the Information Commissioner's Office. We will advise the customer that we will no longer enter into any correspondence about such cases, unless material new information becomes available.

Each case will be considered on an individual basis. The decision to classify a customer unreasonable will be made by the Head of Service and logged on the unreasonable customer behaviour register. The customer will be informed of this in writing by the Head of Service of the department logging the incident.

Options for action

Restrictions will be tailored to deal with the individual circumstances and may include one or more of the following (the list is not exhaustive):

1. Refusing to register and process further complaints/requests about the same or similar matters
2. Requiring the customer to make contact by telephone only through a third party for example solicitor/councillor/friend acting on their behalf
3. Requiring any personal contacts to take place in the presence of a witness and in a suitable location
4. Placing limits on the number and duration of contacts with staff
5. Offering a restricted time slot for necessary calls
6. Limiting the customer to one method of contact (telephone, letter, email, etc.)
7. Requiring the customer to communicate only with one named member of staff

Who decides what incidents or risks are entered onto the registers?

Entries on the Customer Behaviour and Incident Register (CBIR) can only be based on either a specific incident or an expression of clearly identifiable concern by a professional and not on general opinions or hearsay. Each entry should pose a genuine risk to staff.

The Corporate Health and Safety Manager makes the initial assessment on receiving the Customer Behaviour and Incident Form and if the incident or risk is serious enough (ie a level 2 or 3) an entry can be added to the register immediately. A full review/risk assessment through the CBIR procedures will then follow.

Risk Levels

To help identify the level of severity of the risk to staff and the appropriate control measures the following risk levels have been created, these are:

Level 1 - Low risk. *Unpredictable behaviour causing fear of an assault or uneasiness*

Examples of behaviour or of disclosed information that MAY attract a level 1 risk include:

a) Aggressive and threatening personal comments about staff members made by telephone, letter, email or using social media.

b) Abusive behaviour which seeks to harass, verbally abuse or otherwise intimidate our officers. This can include the use of foul or inappropriate language or the use of offensive and racist language

c) Known substance misuse where there is evidence that the abuse of the substance can result in changes in behaviour that may pose a risk to staff.

d) Known needle stick risk in property. This reflects the risk of needles being disposed of improperly even where the use of needles is for a legitimate purpose.

e) Vexatious and malicious complaints/allegations made towards or about staff.

Level 2 - Medium risk. *Abusive behaviour, including threats of physical violence*

Examples of behaviour or of disclosed information that MAY attract a level 2 risk include:

a) Threatening behaviour including personal threats to harm. This may include serious threats issued by the subject towards neighbours or officers in other agencies.

b) Previous unspent convictions for violent and sexual offences disclosed by the customer, Police or Probation services. These include: Common Assault and Sexual Assault (where there is no violence involved).

c) Having been identified by another agency as presenting a risk to staff (and we can substantiate that information as being accurate).

d) Displaying behaviour that may indicate a mental health problem that is a potential risk to staff safety.

Level 3 - High risk. *Actual or attempted physical assault*

Examples of behaviour or of disclosed information that MAY attract a level 3 risk include:

a) Specific incidents of violence or attempted violence demonstrated by the subject towards council officers, neighbours or officers working for other agencies (where this can be substantiated).

b) Disclosed previous unspent convictions for serious violent and sexual offences. These include:

- Sexual assault where violence has been used
- Assault with intent
- Actual bodily harm
- Grievous bodily harm
- Knife and firearm offences

(This is not an exhaustive list and further offences could be considered for inclusion at the discretion of a review group.)

c) Sex or violent offenders on release from prison where the offender management unit suggest this.

d) Where recommended by the Police and/or Probation Service that a person is a risk to members of staff and members of the public and is the subject of ongoing monitoring.

e) Suspected involvement in organised crime gangs (information provided by the Police).

f) Previous unspent convictions for other serious criminal offences involving serious violence and/or the use of offensive weapons, knives and firearms.

An incident should be considered in context so that incidents that meet the criteria for level 2 or 3 risk could translate into a level 1 risk if the circumstances that led up the incident are unlikely to be repeated. Similarly a customer that repeatedly offends at a level 1 may be escalated to a level 2/3 to reinforce the seriousness of their actions.

The Customer Behaviour and Incident Group

To ensure the incidents and information recorded on the register is fair and consistent all report forms are considered by a group of officers who form the Customer Behaviour and Incident Register (CBIR) group. The membership of the group is currently:

- Director of Resources
- Head of Safer Neighbourhoods
- Deputy Elections Manager and FOI/DPA Co-ordinator
- Environmental Protection Manager
- Head of Planning
- Corporate Health and Safety Manager
- UNION Health and Safety Secretary
- Corporate Health and Safety Representatives
- Head of Corporate Governance
- Plus the relevant Head of Service for the incident (if not one of the above)

This group will make a decision on whether an incident is entered onto the register taking into account the following:

- The circumstances of the incident and the nature of the risk
- The degree of violence used or threatened or the nature of the verbal abuse
- Whether it is a repeat offence
- Any opinions or recommendations given by professionals working with the individual
- Any appeal or mitigating circumstances.
- Whether or not the incident indicates an ongoing risk to staff

Customer Services and the System Administrators are notified of the reports as they arrive to avoid any delays then the cases are forwarded to the CBIG core group. A minimum of 3 group

members are needed to make a decision. Once a decision is made an entry is either made by the HR Client Support and Projects Officer on to the register or it is refused and the system administrators are notified. Feedback on the decision of the group is sent to the member of staff and manager that completed the initial report.

What is the register and how is it accessed?

The Customer Behaviour and Incident Register itself is simply a password protected spreadsheet which is kept up-to-date by the HR Client Support and Project Officer through the decisions of the CBIR group.

However, in order to ensure access to this information is as simple as possible, existing departmental case management systems (or similar) are utilised where possible. This involves personal accounts or property databases being flagged or marked in some way by the system administrators so that the staff users can easily identify there is a CBIR entry to be looked at in their own files. This has several benefits:

- One touch access, no searching more than one database
- Access controls are already established
- Confidentiality agreements are in place
- This limits who has access to the full register in compliance with the Data Protection
- Remote access is available.

Each department nominates an administrator and deputy who will ensure their system is updated with any new information entered on the register. How this information is highlighted on each departmental system will vary and may simply be a red marker or other basic notification against a name or property. Administrators will be able to provide additional information about each incident to staff/managers on request and where appropriate, as they have full access to the Register.

What information is recorded on the register?

The following information can be recorded on the register, although in some cases not all will be relevant or available. Access to this personal detail is restricted to the CBIR group and the system administrators and only disclosed on request from an appropriate officer.

- Name
- Address
- Other known addresses
- Date of incident
- Description of the incident (including dangerous structures, dangerous animals, drug usage, weapons ownership)
- Recommended actions
- When the individual is told of the entry or the reason why not
- If shared with CCC partner agencies
- Date for planned review
- Other comments

Data Protection

Under normal circumstances this type of register would not be permitted under the data protection principles as it holds personal and often sensitive information on individuals, which could be seen by staff who would otherwise not need the information to provide a service. However, the Data Commissioner allows the recording of possible risks to staff warning markers in order for an employer to fulfil their duties under the Health and Safety at Work Act 1974. How this information is recorded, accessed, reviewed etc. must be justified and proportionate to the level of risk. The process detailed in this guidance note is written to ensure that these requirements are met.

Notifying the individual

The Data Protection Act expects the council to notify customers who are placed on the Customer Behaviour and Incident Register. The relevant Head of Service sends this letter following the decision of the Customer Behaviour and Incident Register group and it must be sent out within ten working days of the decision. There are two templates available; however these will need to be adapted depending on the circumstances of the incident.

The letter must address the following points:

- The nature of the threat or incident that led to the entry.

- That a record of the incident will appear on a register of risks to staff.
- How services will be provided to them while the entry is current if appropriate.
- Who we may pass the information to.
- When the decision will be reviewed.

There may be cases where we believe informing an individual would in itself create a substantial risk, perhaps of a violent reaction, either towards staff, family members, dependants or others. This could be as a result of emotional instability or a mental health condition. Where this is deemed likely by the group, notification won't be sent and the justification for this decision will be documented on the register.

Review

To ensure the register is administered fairly and information not kept for longer than is necessary each entry must be reviewed. The standard review period is 36 months from the date of entry, but this may be varied according to the risk. If a subsequent report is received within this time period an immediate review will be carried out. All reviews are carried out by at least 3 members of the CBIR group who will recommend that the entry be retained or removed, based on whether:

a) There is objective evidence that there is no longer an on-going risk the entry will be removed.

b) There is objective evidence that there is an ongoing risk the entry will be retained for a further 36 months (unless a shorter period is agreed). This may include an increase or decrease in the level of controls recommended.

The review of each entry will consider:

- Any information provided by staff (good or bad) on contacts had with the individual since the incident or concern was raised.
- The severity of the original incident or concern.
- How services are currently provided to the individual.
- Any representation made by the individual identifying any extenuating circumstances.
- Information made available from other organisations relating to the individual or other incidents.
- Representations from staff.

During the review process the CBIR group need to be able to justify whether an individual remains a credible risk to staff. Essential to this process is information detailing the experiences staff have had with the individual since their entry on the register or since the last review.

The HR Client Support and Projects Officer will notify the administrators when a review is coming up on an individual and ask for any available information held on their system relating particularly to behaviour since the last review date or entry onto the register.

Passing information to other organisations

The council can't share information with other organisations unless there is a credible risk of an unlawful act, such as an assault on their staff. The decision to share will be on a case-by-case basis and only with organisations working in partnership with or on behalf of the council.

Users must not give information from the register to other organisations without authorisation. An initial request must be made in writing to the Customer Behaviour and Incident Register Group. If appropriate, information will be provided in writing to a senior officer in the receiving organisation. Details of the information shared, when and with who are entered onto the register. If an entry on the register is changed or removed all organisations with whom the information has been shared will be informed.

When individuals are made aware of their inclusion on the register the letter will also explain that the council may also share this information with organisations that work for and on behalf of the council.

Using information from other organisations

Information from other organisations can be used to create an entry on the register. To do this the usual Risk Entry Form should be completed and submitted. Consideration needs to be given to how the providing organisation manages this information, for example frequency of review and notifying the individual. Once an entry is made using external information it will be

reviewed on an annual basis as already described. This review will involve contacting the organisation providing the information to confirm any changes or further incidents.

New complaints or requests for information

We will not ignore unrelated service requests or complaints from customers who are classified as unreasonable on the register. The service manager will decide whether any restrictions which have been applied are appropriate and necessary in relation to the new complaint or request.

Referring cases to the Local Government Ombudsman and Information Commissioner's Office

There may be circumstances where either the council's internal complaints process has been exhausted or matters need to be expedited. In these cases the Head of Corporate Governance may seek to close the case without completing all stages of our complaints policy, or we may expedite the case to a final stage. If this becomes necessary, the Head of Corporate Governance will advise the customer of the reasons for this and the options open to them.

Similarly, we may also liaise with the Ombudsman or the Information Commissioner and ask them to consider a case before it has exhausted our complaints/FOI process. It will be entirely at the discretion of the Ombudsman or Information Commission whether or not they accept the referral.

Record keeping

Records of any decisions relating to the CBIR will be retained by the HR Client Support and Project Officer in the Finance team. Under GDPR we are under a duty only to retain what is necessary, which for this purpose is:

- Name and address of the customer
- Details of each request or incident classified as unreasonable or vexatious
- The restrictions that have been put in place
- The date restrictions were put in place, along with review and expiry dates.

Appendix A: Local Government Ombudsman and Information Commission Definitions

Local Government Ombudsman definition of unreasonable behaviour:

We have simplified the Local Government Ombudsman's definition of 'Unreasonable complainant behaviour' as the basis for our definition.

Ombudsman definition:
Unreasonable and unreasonably persistent complainants are those complainants who, because of the nature or frequency of their contacts with an organisation, hinder the organisation's consideration of their, or other people's, complaints.'

Information Commissioner's Office definition of a vexatious or repeat request:

We have adopted the Information Commissioner's Office guidance on 'Vexatious and Repeated Requests' as the basis for our definition:

Information Commissioner's Office guidance:

Vexatious - 'Deciding whether a request is vexatious is a flexible balancing exercise, taking into account all the circumstances of the case. There is no rigid test or definition, and it will often be easy to recognise. The key question is whether the request is likely to cause distress, disruption or irritation, without any proper or justified cause.'

Repeat requests - Where a public authority has previously complied with a request for information made by any person, it is not obliged to comply with a subsequent identical or substantially similar request from that person unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

The Freedom of Information Act 2000 gives rights of public access to information held by public authorities. However, Section 14(1) of the Act protects public authorities from those who might abuse the right to request information.

If a request is vexatious or repeated, we do not have to provide any information, or confirm or deny whether we hold it (however we will issue a refusal notice).

When the decision has been taken to classify a customer's behaviour as unreasonable or to classify a request as vexatious, the Customer Contact Manager will write to the customer to:

- Detail what action we have taken and why
- Explain what it means for the customer's contacts with the organisation

- Advise how long the restrictions will last and when the decision will be reviewed
- Enclose a copy of this procedure for the customer's information

Further ICO Guidance is available on their website https://ico.org.uk/

--End--