Customer Identification and Verification Policy

Serving people, **Improving lives**

Document control	
Document title: Customer Identification and Verification Policy	
Version number: 1:0	**Author**: Lizzy Gregory, Assistant Director, Customer Engagement
Date approved:	**Approved by:**
Effective date:	**Document status:**
Superseded version: N/a	**Date of next review:** 07/2027

Gedling Borough Council

1.0 Introduction

The Council is committed to ensuring that it securely manages personal, special category and confidential data and only discloses such data to customers and other third parties when the appropriate checks are performed to verify the customer's identity or authority to receive the data. The Council will only disclose personal, confidential or special category data in accordance with data protection legislation and any other relevant legislation and takes breaches of data protection and confidentiality seriously.

For the purposes of this policy, data means personal, special category or confidential data.

This policy covers all customer-interactions with the Council. In accessing some Council services there may be separate Identification and Verification (ID&V) checking procedures which require additional higher levels of verification (for example where the customer must provide paper documents, complete CRB checks or presenting in person for tests, such as taxi driver knowledge checks). Where there is a separate route of ID&V checking this will be clearly set out below.

A clear and accessible ID & Verification process and policy allows the Council to demonstrate its commitment to managing customer data securely and only disclosing data to those customers who are correctly verified. If a customer feels their data has not been protected and the council is not abiding by these guidelines, they are able to escalate a complaint to the ICO Information Commissioner's Office (ICO)

The purpose of this Policy is to ensure that:

- The council manages access to data lawfully.
- The council takes the right steps to verify a person before disclosing data held on them or makes changes to this data (including taking payments, feedback/complaints).
- Officers are aware of the types of information that can be used for ID&V purposes.
- Officers are aware of their obligations to ensure ID&V has taken place before data is released.
- Officers know what to do when a data breach occurs
- Managers are aware of their obligations for ensuring their reports are carrying out correct ID&V checks prior to releasing information or acting on a customer's behalf.
- Officers are aware of the correct procedure for verifying third parties before dealing with that party about another customer's account.
- Credibility and accountability are maintained through meaningful review and monitoring.

2.0 Definitions

For the purpose of this Policy 'Identity and Verification' will be referred to as 'ID&V', any person dealing with the Council to access information or make changes to information we hold on them or make payments, will be referred to as the 'customer'. Any officers dealing with these customers will be referred to as 'officers'. Customer Relationship Management System is the computer system that customer services use to enter customer and case information and will be referred to as 'CRM'.

For the purposes of this policy, data means personal, special category or confidential data.

3.0 Authenticating a customer

When a customer calls and requests access to information about them or someone else or wants to make a change or update the information held on them, officers should always take steps to verify that the identity of the customer is the person whose information they will be accessing or

providing (or where they are calling on behalf of a third party, that officers verify they have permission to access that customers information). We call this process ID&V (or identity and verification). Officers must perform ID&V on all customer contacts before providing information which would be considered personal/protected information.

This guidance will help officers choose the right method of ID&V to be used depending on the customer, service and the situation. This ID&V could take the form of them providing an account code that we hold for them, their personal information or a password.

3.1 What is personal information Special category Information and Confidential Information?

Personal information is any information relating to an identified or identifiable natural person, An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as name, and identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, cultural or social identity of that natural person.

Types of personal information include but are not limited to:

- •Name and address
- •Email address
- •Employment details
- •Date of birth
- •Bank details
- •Income level
- •Marital status
- •Account information
- •Image on CCTV
- •Description of a person
- •Photographs
- •Expressions of opinions
- •Emails
- •IP Address
- •Online usernames
- •Identification numbers
- •Profile information
- •Usage data

Special Category Information
Special Category Information refers to personal data that is considered more sensitive and therefore requires additional protection under data protection legislation. This includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (where used for identification purposes), health data, or data concerning a person's sex life or sexual orientation. Processing this type of data is subject to stricter rules because of the potential for greater impact on an individual's privacy and rights.

Confidential information

Confidential information refers to any data or details that are private, sensitive, or not intended to be shared publicly. This can include personal data, financial records, internal communications, or any information that, if disclosed without appropriate authorisation, could compromise an individual's privacy or the interests of an organisation. Such information must be protected and only shared with those who have a legitimate need to know, in accordance with relevant data protection laws and Council policies. If officers are unclear about what might amount to confidential information they should seek advice from legal services. Confidential information is not limited to personal data.

3.2 When are ID&V checks required and not required?

If a customer is calling to make enquiries that **do not require the officer to disclose data** (for example where to find something on our website, opening times of our leisure centre, reporting fly tipping anonymously or requesting contact details for a councillor) **ID&V checking is not required.**

If at the start or during an interaction with a customer they request the disclosure of / or changes

to, personal or restricted information we hold about them or cases logged on our system that relate to them, this is a situation within which **ID&V checking must be done** before any data is disclosed to the customer.

For example,

- a customer rings asking how much their next council tax payment will be,
- a customer wants to find out what is happening with their housing application
- a customer calls on behalf of their disabled partner to change their address on our system.

3.3 Checking the identity of a customer before providing information

When a customer contacts the council, either in person, over the phone or in writing (letter, email, chat, text etc). We should ensure that we are dealing with the right person before providing any information or taking any action on that customer (or a third party) account. This includes adding case notes, updating information, taking payment etc.

Officers should advise customers, that before being able to assist them with their enquiry it is the policy of the council that we must perform some checks to ensure they are dealing with the correct person and have authority to proceed.

Officers should attempt to verify the customer against several verification methods (see section 5.0) depending on the type of call and what is held on file for the customer.

Some methods of verification might be easier for the customer to provide than others, but officers should try and ensure the verification methods officers use give a high level of confidence of the customer's identity before continuing with the call and if officers are not confident they are speaking to the customer held on file from the information provided, they should not proceed and instead ask the customer to gather this information and contact the Council back.

In relation to ID&V on written correspondence please see section 7.0.

3.3 Customer not wanting to have their personal details recorded, but requesting information

If a customer requests to receive an update on a case, they have logged but have not provided any of their personal details, it will not be possible to identify or verify them. In this situation, the officer should ask the customer for the case number or details of the case (fly tipping at a specific location, noise request at a specific address). If the customer can provide this detail the officer can give them general information about the case being logged and details about any follow-up but should not provide any personal details or information that may be confidential. E.g. who else reported the case, what another person has said about the case, information about an outcome that is not official yet. If an officer is in doubt as to what information should be provided, they should contact their manager for advice. If the enquiry relates to a sensitive matter (e.g. Homelessness etc.) then no case data should be shared with the customer to avoid putting the reporter at risk.

4.0 Customer ID

Some customers will be able to access their account information online and where possible, we should always encourage them to do so as this password protected access can provide the highest level of security for the customer and protection for unwanted changes to their data.

Through their online account customers will be able to link their own data by providing authentication to join their information together.

4.1 Different types of ID&V

There are different types of ID&V a customer may be able to provide, and different types will be appropriate and applicable depending on the situation:

- **Personal information**: information relating to who the person is and the details they know about themselves

- **Transaction details**: information about payments or refunds the person may have had into their personal or business bank account

- **Customer location/property:** details relating to a customer or businesses location or assets they own which may include vehicles/taxis, registration details (Business, charity)

- **Council provided ID:** These are reference numbers provided by the council to the customer, they may be issued verbally or in documentation sent through the post, text or email. They include customer reference numbers for benefits, council tax, planning and customer and case numbers issued through the CRM.

- **Third party verification:** Where a customer calls on behalf of another, the customer should provide evidence of their authority to receive data. They may have a power of attorney to discuss the customers information or verbal or written consent may have been given by the authenticated customer on the call or previously and recorded on file with the details of the third party authorised to discuss the account. The duration for how long third-party authorisation applies should also be noted. For information about dealing with information relating to a child, please review section 7.2.

5.0 Completing ID&V successfully.

To successfully verify a customer, an officer, depending on their service and the type of enquiry, must collect identity information as prescribed in the table from the lists noted below (A,B,C,D,E) *(note: if the employee can obtain more than the number of pieces specified below, this is more secure and should be recorded):*

Service area	The customer must provide:
Council Tax	**2** items from list A **and** at least **1** from list B **OR 1** Item from list A and 2 from B **ALSO must** include 1 item from list C
Business Rates	**2** items from list A **and** at least **1** from list B **OR 1** Item from list A and 2 from B **ALSO must** include 1 item from list C
Benefits	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Elections	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Waste	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Environment	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Housing	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Payments/Cash Path	**2** items from list A **and** at least **1** from list B or D **ALSO must** include 1 item from list C
Licensing	**2** items from list A **and** at least **1** from list B **ALSO must** include

	1 item from list C
Planning/ Building control	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Leisure	Before providing any protected information around a customer's details or a case held on the system the officer should verify the customer **2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C. **Where the enquiry involves a child or third party, they should use list E**
Cemetries	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Public Protection	**2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C *(verification from both list B and C should be acquired where possible and specifically where information is being given which may be inadvertently divulged to a third party).*
HR/Finance/ internal dept	Someone calling seeking information relating to theirs or another person's employment records should be referred to the HR department for review.
Customer Services	If the call does not fall into one of the categories above or the enquiry is unclear, before providing any protected information around a customer's details or a case held on the system the officer should verify the customer **2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C
Someone calling on behalf of another/third party (not a child)	The officer must ensure the correct customer record is being accessed with **2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C, to verify the identity of the customer being enquired about and **must verify the caller's authority** to discuss by using **list E**.
Someone calling on behalf of their child	The officer must ensure the correct customer record is being accessed with **2** items from list A **and** at least **1** from list B **ALSO must** include 1 item from list C, to verify the identity of the customer being enquired about and **must verify the caller's authority** to discuss by using **list E**.

6.0 Receiving a transferred call

If an officer receives a call transferred from a colleague within the Council, **they should not assume that ID&V checking has already been performed** by the previous officer unless this is explicitly stated as part of the call handover and recorded on the CRM. If ID&V has not been done, the officer must proceed to complete ID&V checking before providing any data. If the customer is upset by having to complete these checks, the officer should reassure them this is necessary to protect their privacy and security of their information.

7.0 Dealing with customer requests in writing

If an officer receives a customer request via email, letter, chat, or any other written media, they should complete ID&V checks with the individual if they are requesting access to data that we hold on them or others. This ID&V check may be achieved by various methods: by using the tables in this process and either calling the customer and asking the questions over the phone, by writing to them and requesting evidence to be sent in (responses to questions not actual ID documents) or asking the customer to come in and they can answer the ID&V questions in person. The officer should be satisfied that the customer has met the ID&V conditions before providing any data to them.

Note: *the officer should check that the written content submitted does not already contain the information needed to complete the ID&V check. E.g. a customer writes to you and includes their*

*name, address, postcode, date of birth and council tax number**. If the information needed to satisfy the ID&V check is provided within the original written content, then the information can be submitted to the customer without additional checking.***

8.0 Dealing with reports made on behalf of another person (one off)

If a person contacts the Council and wants to make a report on behalf of another person, after verifying the customer's identity, the officer can ask the details of the person they want to make the report under and record this under the customers record on the system (CRM or other system). Officers should note that this report was made by another person (and record details of who made this report) and not the customer in the detail on the system. If the other person wants to access information held by the council on the customer, this should not be provided without express permission from the customer (refer to list E). ***The CRM will flag that a report has been made by a third party and when the customer calls, this report should be checked with the customer to ensure they are happy with the contents of the report and that it remains on their record.***

8.1 Parent/guardian acting on behalf of their child

The ICO guidelines state 'If you're asked for personal data about a 12-year-old (plus) by their parent or carer, you should usually get permission from the child first'. If a parent/guardian is requesting information in relation to a child, officers should go through ID&V to ensure that the parent/guardian's identity is verified and that they are sufficiently knowledgeable about the child's details before providing information we hold on the child. If a child contacts the council to request that their parent/guardian should not be allowed to access their information, this should be recorded on the child's file (and on the CRM) and further requests to access the child's records should be denied. The child must be informed that their parent/guardian will be told that the child has requested the parent not to be able to access to records upon request. Any appeals from the parent should be referred to the legal department.

8.2 Calls from councillors

If a councillor is calling and expresses that they have been given permission by the customer to speak on their behalf and provide personal details, this should be recorded on the customer's record on the CRM and details of the councillor calling to report the problem. If the Councillor wants to receive data on behalf of the customer they should provide confirmation of the customer's consent to share the data. If a customer calls to follow up on their councillor reported case, councillor reporting should be discussed with them and authorisation to keep the councillor updated as to the case progress should be taken and recorded on the customer record. If the customer expresses that they did not give the councillor access to their personal information or to report this case on their behalf, **this should be escalated to the legal department for review.** ***The CRM will flag that a report has been made by a third party and when the customer calls, this report should be checked with the customer to ensure they are happy with the contents of the report and that it remains on their record.***

9.0 Monitoring how customers use our service

As well as making sure officers verify the customer prior to accessing or changing details on the account, officers should ensure that they check the customer's account and highlight with them (after successfully completing ID&V) any recent changes made on their account that may be suspicious (such as third-party access, unrecognised payments, address differences) and work with the customer to ensure any updates to the account or deletions of connected accounts are completed promptly to keep access to the record secure.

10.0 If a customer reports unauthorised access to their account/information

If a customer makes contact and reports that someone has made changes to their details or has noticed anything suspicious in their communication with the Council, employees should reassure the customer that they will investigate the activity. A note should be added to the customer file detailing this whilst the investigation takes place to ensure no further access breaches occur. Officers must first ID&V the customer and go through their account and check for any details which look incorrect or suspicious. In the event that something suspicious is found they must complete the data breach form (policy and form are here). If officers identify any suspicious or unrecognised activity this should be documented on their account and a case raised with the employee's manager and the Data Protection Officer as a potential data breach using the council's 'data breach reporting procedure'.

11.0 Managers monitoring ID&V adherence

Managers in every customer facing service must have a process in place for periodically monitoring a sample of employees' interactions with customers and ensuring correct ID&V checks are carried out every time. Where these checks are not carried out with a customer prior to disclosing information or making changes on the account, this may amount to a data breach and will be a failure to comply with this policy document. The manager may choose to put additional monitoring in place and may proceed through a disciplinary process with the affected employee. Please consult HR should additional advice on how to proceed be required.

12.0 Complaints about how we manage customers information and ID&V checks

These should be raised in line with our complaints policy and if a data breach is raised by a customer by way of complaint, this should be reported to the Data Protection officer for review.

13.0 Referring to the Information Commissioner's Office (ICO)

Where the customer insists that a serious breach has occurred or the manager or Data Protection Officer identify this, a case may be escalated to the ICO by the Data Protection officer in line with the procedure set out in the Council's Information Security Policy here (Information security incident management section). **No individual service should contact the ICO directly.**

The ICO identifies a breach as:

UK GDPR data breach reporting (DPA 2018)
If any personal data that you're responsible for has been lost, accidentally destroyed, altered without proper permission, damaged or disclosed to someone it shouldn't have been, this could be a personal data breach.
The scope of the breach and how you handle it could have serious consequences for the people who are identifiable in the data. In some cases, personal data breaches – once discovered – have to be reported to the ICO within 72 hours.

14.0 Exclusions to this policy

In some instances, the customer may need to undergo additional ID&V checks or provide specified information when dealing with special applications/changes or checks, they may need to provide different ID verification. Some of these situations are laid out below but should not be considered exhaustive and should be checked with employee's manager.

- Taxi driver licensing (in person verification of photo ID against person)
- CRB checks for people working with vulnerable customers (in person completion of CRB form and address history, photo ID provided)

- Employee HR checks
- Councillor ID checks
- Housing Needs applications
- Council Tax/Housing Benefit
- In response to a Subject Access Requests

Councillors may be entitled to receive data about a customer as part of their role, the passing on of such information is outside this policy but within the Councils Data Protection Policies.

Appendix A

List A - Personal information

Evidence type	Details
Customer name (checked on CRM)	Matches what is detailed on council systems (including CRM) or official documentation held on file passport, driving license etc.
Date of birth	Matches what is detailed on council systems (including CRM) or official documentation held on file passport, driving license etc.
National Insurance number	Matches what is detailed on council systems (including CRM) or official documentation held on file passport, driving license etc.
Email address	Matches what is detailed on council systems (including CRM)
Mobile/ home phone number	Matches what is detailed on council systems (including CRM) or official documentation held on file, phone bill etc.
GP details	Matches what is detailed on council systems (including CRM) or official documentation.

List B – Customer/Business location/property

Evidence type	Details
Address incl. postcode	Matches what is detailed on council systems (including CRM) or official documentation held on file utility bill, council tax bill etc.
Registered business/charity number	Matches what is detailed on council systems (including CRM) or official documentation held on file companies house certificate, companies house website, company/charities own website.
Business telephone number	Matches what is detailed on council systems (including CRM) or official documentation held on file companies house certificate, companies house website, company/charities own website.
Business address	Matches what is detailed on council systems (including CRM) or official documentation held on file companies house certificate, companies house website, company/charities own website.
Business name	Matches what is detailed on council systems (including CRM) or official documentation held on file companies house certificate, companies house website, company/charities own website.
Vehicle licence plate number	Matches what is detailed on council systems (including CRM) or official documentation VO5 logbook, DVLA, taxi license plate.

List C - Council provided ID

Evidence type	Details
Account number	Matches what is detailed on council systems (including CRM) or official documentation bank statement, banking app.

Invoice number	Matches what is detailed on council systems (including CRM) or official documentation held on file.
Case number	Matches what is detailed on council systems (including CRM).
Complaint ref	Matches what is detailed on council systems (including CRM).
Benefit ID	Matches what is detailed on council systems (including CRM) or official documentation held on file or official benefit paperwork.
Leisure centre membership	Matches what is detailed on the council systems (including CRM) or official documentation held on file.
Taxi driver reference number/ badge number	Matches what is detailed on council systems (including CRM) or official documentation held on file.
Benefits claim number	Matches what is detailed on council systems (including CRM) or official documentation held on file.
Council tax number	Matches what is detailed on council systems (including CRM) or official documentation held on file.
Electoral roll number	Matches what is detailed on council systems (including CRM) or official documentation held on file or from the electoral roll website.
Taxi badge number	Matches what is detailed on council systems (including CRM) or taxi badge or official letters held on file.
Planning reference number	Matches what is detailed on council systems (including CRM) or council planning documentation.
Housing reference number	Matches what is detailed on council systems (including CRM) or official documentation from benefits, housing provider, other councils etc.
Booking number	Matches what is detailed on council systems (including CRM) or leisure/booking systems.
Password	If the council has provided a password to access the customer account, this can be used if matches what is recorded in the council system.

note – if a customer is unable to access any of the reference numbers provided by the council in list C and there is no way of them obtaining these, the case should be referred to a manager to review. They can permit disclosure of customer information only in exceptional circumstances and this must be noted on the customer case records by the manager as to why and what level of assurance we have that the customer is authenticated by other means.

List D - Transaction details

note, if customer making a payment, must confirm it is their own card they are using. Customers are permitted to make payments on behalf of another customer, but they must know the details of the account they are paying into, and officers should not disclose customer information to a third party unless they have passed third party verification (see below).	
Last payment amount	As detailed on our CRM system or other council systems or receipts.

List E – Calling on behalf of another details

Evidence type	Details
Power of attorney documentation	Officers should record the document ID number, how long the power of attorney applies, if no date noted, should detail that the

	document should be rechecked a year from the call.
Verbal authority provided by the customer on the call	If an officer speaks to the customer who confirms their identity and gives permission for another person to speak on their behalf and be provided information about them, that should only apply for the duration of that call only. Should the third-party call back and request further information, permission must again be gained from the customer.
Parent/Guardian on behalf of a child	A parent/ guardian should be able to provide proof of guardianship. This may come in the form of confirming the child's DOB, address, other parent/guardian, what sessions/appointments they attend, or last payments made to council.
Signed declaration	Letter from the customer detailing authorisation for the named person to act on the customers behalf. This letter must be dated within 6 months and contain the customer's name, address, telephone number and where possible the customer should be contacted to verify the letter is genuine