CASH ACCESS UK PRIVACY NOTICE

Version	4.0
Effective Date	November 2026
Policy Owner	Chief Operating Officer
Last Review Date	November 2026
Next Review Date	November 2027

1. Purpose

Cash Access UK Limited (**Company**) is responsible for the operation of banking hubs used by its members (each of which is a UK bank or building society) to ensure that customers continue to have access to cash and in-person banking services.

This privacy notice applies to personal data about you which is used by the Company only and does not apply to personal data about you which is used by your bank or building society. Your bank or building society will have a separate privacy notice for this, which you can request from your bank directly either via their website, their customer support services, or from your banker in person.

The Company respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when you interact with us, such as when you visit one of our banking hubs, visit our website or when you call us. This notice tells you about your privacy rights and how the law protects you.

2. Introduction

Purpose of this privacy notice

This privacy notice aims to give you information on how the Company collects and processes your personal data.

It is important that you read this privacy notice carefully so that you are fully aware of how and why we are using your data.

Who we are and who this notice applies to

We are Cash Access UK Limited and we are responsible for the operation of the Access to Cash programme. We are referred to throughout this notice as the **Company**, **we**, **us** or **our**.

We are the controller of, and we are responsible for, the personal data of:

- individuals who visit any of the banking hubs we operate and are recorded on our CCTV systems when they visit a banking hub;
- individuals who provide feedback or take part in any surveys or community engagement we are involved in;
- individuals who call us via our public facing phone number.
- individuals who make a complaint to us;
- individuals who visit our website at www.cashaccess.co.uk;
- business contacts that we deal with on a day-to-day basis, such as employees or representatives of our suppliers, the banks we work with, our professional advisers, and regulators; and
- individuals who apply for jobs with us.

We have appointed a data protection officer (**DPO**) who is responsible for overseeing questions in relation to this privacy policy. If you have any questions about this privacy policy, including any requests to exercise your legal rights, please contact the DPO using the details set out below.

Contact details

If you have any questions about this privacy notice or our privacy practices, please contact our

DPO by email at: DPO@istormsolutions.co.uk

Your right to complain

You have the right to make a complaint about the way we handle your personal data at any time to the ICO, the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us using the details above in the first instance. If you are unhappy with the way we handle your complaint, you can then raise the matter with the ICO.

Changes to the privacy notice and your duty to inform us of changes

We keep our privacy notice under regular review. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

3. Data we collect

Data Categories

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).
We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

Identity Data includes first name, last name, username or similar identifier, marital status, title, date of birth and gender. This may be collected when you fill out a form, such as a survey, or if you correspond with us on any matter.

Contact Data includes postal address, email address and telephone numbers, including the professional contact details of our business contacts. This may be collected when you correspond with us on any matter.

CCTV Data includes images and footage recorded by the CCTV systems at our banking hubs, which may capture you if you visit any of our banking hubs. This is collected by our CCTV systems when you visit a banking hub.

Incident Data includes information that may be recorded if you have an accident or if you are involved in any incident in one of our banking hubs. This may be collected by personnel in the banking hub and recorded by them on applicable systems, and CCTV Data.

Recruitment Data includes any personal data you may give to us as part of a recruitment process, including your Identity Data, Contact Data, your CV and your responses to application form questions or assessment questions. For some roles we may also be required to run a credit check and / or a disclosure check against you, however you will be informed if this applies to you. This may involve the collection and use of information about criminal convictions and offences. This may be collected when you apply for a vacancy and may include information provided to us by third parties in the context of a credit check and / or a disclosure check (where applicable).

Feedback Data includes any opinions or feedback you may have about our banking hubs or the work we do which you provide to us, such as when we conduct a survey or a community engagement exercise (or if you otherwise contact us with your feedback). This may be collected when you complete a survey or otherwise provide us with feedback, or it may be provided to us by a third party where you have given them feedback about our banking hubs or services.

Complaints Data includes any complaints you may make about our banking hubs or the work we do. This may be collected when you file a complaint against us, or it may be provided to us by a third party where you have given them feedback about our banking hubs or services.

Website Data includes:

Technical Data includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.

Usage Data includes information about how you use our website and any online surveys or facilities available on our website.

This is collected when you visit our website and may include data provided by analytics providers (such as Google Analytics).

Communications Data includes your communication preferences. This may be collected when you fill out a form, such as a survey, or if you correspond with us on any matter.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose (such as evaluating the effectiveness of our banking hubs) with our stakeholders. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will **not** directly or indirectly reveal your identity. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy policy.

We may collect **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health, and genetic and biometric data) as part of an Incident Data or CCTV Data, or if you provide this to us as part of your Feedback Data or in your

Complaints Data. Special category data and data about criminal convictions and offences may also be collected as part of Recruitment Data.

Please note we do **not** collect or receive financial or transactional information about the banking services that you may access or receive in any of our banking hubs. This information is held by the Post Office and your bank, who provide these services from our banking hubs. We only receive Aggregated Data (as defined above) regarding transactions processed in our banking hubs so that we can monitor use of each banking hub and report on this to our regulators.

If you fail to provide personal data:

All of our banking hubs have CCTV in operation, and so you will not be able to visit a banking hub without being recorded by our CCTV systems.

We may also be required by law or for defending or pursuing a legal claim to collect and record certain personal data about you, for example if you are involved in an accident or incident in one of our banking hubs.

Otherwise, if you decide not to provide your personal data to us, you may not be able to engage with us, provide feedback or use our website.

4. How we use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us using the details above if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

CASH ACCESS UK PRIVACY NOTICE

Purpose/Activity	Type of data	Lawful basis for processing
Business-as-Usual Communications: We may collect and use personal data as part of our business-as-usual interactions with employees and representatives of our stakeholders, regulators and suppliers.	Identity Data Contact Data	Necessary for our legitimate interests to develop banking hubs and to ensure proper management of operational banking hubs
CCTV: We operate CCTV in our banking hubs which records everyone visiting a Banking Hub.	CCTV Data	Necessary for our legitimate interests to ensure the security of our banking hubs CCTV footage may also be used or shared with third parties where necessary for the prevention and detection of crime, apprehension of offenders, or in the establishment, exercise or defence of legal claims
Surveys and feedback: We may collect and use personal data where this is provided to us as part of any survey, feedback or community engagement exercise.	Identity Data Contact Data Feedback Data	Consent may be obtained as part of any formal survey or community engagement exercise, or data is otherwise provided voluntarily Necessary for our legitimate interests to receive feedback on the banking hubs and services we provide, to enable us to improve banking hubs and services and make key strategic decisions regarding where to establish banking hubs

Purpose/Activity	Type of data	Lawful basis for processing
Phone calls: We may collect and use personal data where this is provided to us as part of any phone call about any of our banking hubs, website or other services we provide.	Identity Data Contact Data Feedback Data Complaints Data	Consent may be obtained as part of any phone interactions, or data is otherwise provided voluntarily Necessary for our legitimate interests to receive feedback on the banking hubs and services we provide, to enable us to improve banking hubs and services as well as address feedback provided.
Complaints: We may collect and use personal data where this is provided to us as part of any complaint about any of our banking hubs or services we provide.	Identity Data Contact Data Complaints Data	Consent may be obtained as part of any formal complaint, or data is otherwise provided voluntarily Necessary for our legitimate interests to receive feedback on the banking hubs and services we provide, to enable us to improve banking hubs and services

Purpose/Activity	Type of data	Lawful basis for processing
Accident or Incidents: We may collect and use personal data about you if you have an accident or are otherwise involved in any incident at one of our banking hubs.	Identity Data Contact Data Incident Data	To comply with legal obligations under health and safety regulations Necessary for our legitimate interests to ensure safety in our banking hubs and to facilitate appropriate responses and resolution of any incident, including as may be relevant for processing any insurance claims Consent may be sought where special category personal data is required, or this may otherwise be needed for the vital interests of the individual Necessary for the establishment, exercise or defence of any legal claims
Website: We may collect and use personal data to administer our website, (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data) and to measure the effectiveness of our website	Website Data	Necessary for our legitimate interests to ensure our website is secure and being used appropriately and to learn from how our website is used in order to identify improvements Consent may be sought to the placing of cookies or other tracking technologies on your device to enable us to collect Technical Data and Usage Data.

Purpose/Activity	Type of data	Lawful basis for processing
Recruitment: We may collect personal data as part of our recruitment process.	Identity Data Contact Data Recruitment Data	Necessary to comply with employment laws which apply to recruitment processes Necessary for taking steps with a view to entering into an employment or similar contract Necessary for our legitimate interests to ensure our employees are suitable for vacant positions
Governance Reporting and Audits: The personal data we hold may be shared with our stakeholders or regulators as part of any audit or governance reporting that we are required to complete under applicable laws and regulations.	All Data Categories	Necessary to comply with applicable laws and regulations relating to the Access to Cash programme Necessary for our legitimate interests to comply with any contractual obligations in place with our stakeholders

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us using the details above.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with this notice, where this is required for the purposes stated in this notice or permitted by law.

5. Website

Third-party links

Our website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see the Cookies Policy on our website at www.cashaccess.co.uk/cookies.

6. Sharing your personal data

We may share your personal data with the parties set out below for the purposes set out in the table above to the following categories of third parties:

Suppliers: We rely on suppliers (such as our IT services, CCTV services and HR services providers) for our operations and therefore your personal data may be held by them on our behalf or otherwise used by them for the delivery of the Access to Cash programme.

Professional advisers: We may share personal data with our professional advisers where necessary to enable them to advise us on the delivery and operation of the Access to Cash programme, including compliance with any legal or contractual obligations.

Stakeholders: The Access to Cash programme has several stakeholders, including banks, our partners (such as the Post Office and LINK), regulators and consumer interest groups. We may share personal data with them where we are obligated to do so or where necessary for their assessment of the Access to Cash programme. We may also share Complaints Data, Feedback Data and CCTV Data with stakeholders in certain circumstances, such as if a complaint or feedback relates to one of their employees, or if CCTV captures an incident involving one of their employees or customers.

Regulators: We may be compelled to share information with our regulators which could include personal data.

Law enforcement: We may be required to share CCTV footage with law enforcement where they request this from us for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

7. International Transfers

The sharing of personal data with the categories of third parties noted above may involve your data being stored outside of the UK.

Whenever we transfer your personal data out of the UK, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

We will only transfer your personal data to countries that have been deemed under UK data protection laws to provide an adequate level of protection for personal data.

Where we use certain service providers, we may use specific contracts approved for use in the UK by the ICO which give personal data the same protection it has in the UK.

Please contact us using the details above if you want further information on the specific mechanism used by us when transferring your personal data out of the UK.

8. Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

9. Data Retention

How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect of our relationship with you.

To determine the appropriate retention period for personal data, we consider a number of factors, such as: the amount, nature and sensitivity of the personal data; the potential risk of harm from unauthorised use or disclosure of your personal data; the purposes for which we process your personal data and whether we can achieve those purposes through other means; and the applicable legal, regulatory, tax, accounting or other requirements.

10. Your legal rights

What are my rights?

Under certain circumstances, you have rights under data protection laws in relation to your personal data:

Request access to your personal data (commonly known as a **data subject access request**). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data in certain circumstances. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have

processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

If you want us to establish the data's accuracy.

Where our use of the data is unlawful but you do not want us to erase it.

Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims.

You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain services to you (for example, we may not be able to process or resolve your complaint). We will advise you if this is the case at the time you withdraw your consent.

If you wish to exercise any of the rights set out above, please contact us at the details set out above.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. If you decide not to pay any fee charged, we may not be able to respond to your request.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. How to Raise a Data Protection Complaint

Under the Data (Use and Access) Act 2025 (DUAA), individuals must now raise any concerns about how their personal data is handled directly with us first, before contacting the Information Commissioner's Office (ICO).

If you have any questions or concerns about how we process your personal data, or if you believe your data protection rights have not been respected, you can submit a complaint to us using the contact details below:

Data Protection Contact:

iSTORM

dpo@istormsolutions.co.uk

10 John Street

Stratford upon Avon

CV37 6UB

We will acknowledge your complaint and aim to respond within one month. If your complaint is complex or requires more time, we will keep you updated.

Escalating Your Complaint

If you have raised a complaint with us and are not satisfied with our response, or if you believe we have not handled your complaint appropriately, you may then escalate the matter to the Information Commissioner's Office (ICO).

ICO contact details:

Website: https://ico.org.uk/make-a-complaint/

Telephone: 0303 123 1113

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

11. Policy Review

This policy is reviewed at a minimum annually against best practice and any applicable legal and regulatory requirements. Any changes to the policy are approved at the relevant committee as per the Policy Management Standard

Version Control

Version	Date	Author	Change Description	Approved By	Date Approved
3.0	03/11/2025				
4.0	26/10/2026	Chief Operating Officer	Scheduled Review	ERC	26/10/2026
4.0	02/02/2027		Approval required at ARCO		