# Data Audit - March 2026 - Operational Data

| Data Held | Where Held | Retention Policy | Justifiyable - lawful reason to Keep | Reason explained | Date of destruction / deletion | Reason for retention |
|---|---|---|---|---|---|---|
| Hirer Information | On line booking System - Scribe. | Whilst hiring | Yes | Minimal contact details obtained in case of emergencies at PGCC. Hirers sign terms and conditions on booking form which is attached to their hire | Digital records archived after year end audit if no longer hiring. | In order to contact them in case of emergency at the centre or to expedite payment or to discuss breach of terms and conditions |
| Customers | Scribe Accounting | Current + 6 | Yes | Receipts and Invoices to be kept in line with statutory retention policy | Any paper copies of invoices to be destroyed. Retention of digital will be archived accordingly | 7 years of accounts is a statutory requirement |
| Suppliers | Scribe Accounting | Current + 6 | Yes | Supplier and supplier invoices to be kept in line with statutory retention policy | Any paper copies of invoices to be destroyed. Retention of digital will be archived accordingly | 7 years of accounts is a statutory requirement |
| CCTV recordings | On premises in restricted location. Local recording (not on-line) | System overwrites after 6-8 weeks due to space | Yes | Internal and external areas (public areas and office) CCTV footage is used for the prevention and detection of crime, protection of staff, volunteers, visitors and Council property. Supports investigation of incidents, accidents, complaints. Restricted access to footage | System overwrites. Any downloaded footage to be deleted after matter resolved or footage passed on to authorities requesting it | Only if authorities request footage to be kept would we keep footage outside of system retention |
| Volunteer Information including DBS where required. Names, contact details, emergency contacts | Digitally & locked cabinet | Whilst volunteering and up to 2 years after leaving | Yes | Volunteer information is required to safely manage volunteering activities and contact volunteers. DBS checks are only undertaken where volunteers work directly with young people. In line with safeguarding requirements. | Up to 2 years afer volunteering ends. Securely disposed of (deleted/shredded) | Short post-volunteering retention allows for resoluation of any queries, provides references, follow up on incidents or safeguarding matters. |
| Safeguarding Concerns, Disclosures, referrals and related correspondence | Locked paper files, restricted access digital records | Up to 6 years after resolution or longer if required | Yes | Safeguarding records are required to protect children and vulnerable adults, demonstrate appropriate action, and meet statutory safeguarding responsibilities | Destroyed securely once retention period ends. | Extended retention reflects the sensitive and potentially long-term nature of safeguarding matters and the need for accountability |

HEDNESFORD TOWN COUNCIL
GATEWAY TO CANNOCK CHASE

# Data Audit - March 2026 - Operational Data

| Data Held | Where Held | Retention Policy | Justifiyable - lawful reason to Keep | Reason explained | Date of destruction / deletion | Reason for retention |
|---|---|---|---|---|---|---|
| Door entry system security codes or cards for hirers access to Council building | Digital file accessed by authorised officers only. Cards issued are recorded for long term hirers or temporarily issued to daytime hirers. | Whilst access is required | Yes | Door security codes are required to control and restrict access to Council premises, ensuring the safety and security of staff, councillors, volunteers, hirers and Council property. Codes are only issued to authorised individuals and are not shared publicly. Officers cards : access to all areas. Councillors: access to all areas except the Town Council Office | Access removed and codes changed immediately when no longer required or when breached/compromised. Cards not returned to be removed from system to ensure no access. | Information is retained only for as long as necessary to maintain building security. Codes are regularly reviewed and updated to minimise security risk |
| Passwords for system, on-line accounts and services (digital platforms) | Stored digitally in secure folder for Chief Officer / RFO use. Looking at Bitwarden or similar to remove need for document | Until account closed or no further need for access | Yes | Passwords are required to access Council related services and systems securely on-line and to ensure business continuity when officers are away. Individual passwords are not shared or given. Access to shared passwords are limited to authorised officers only and in line with role responsibilites and least-privalege principles. | Passwords are changed, revoked or deleted when access is no longer required, when roles change or when employees with access leave the organisation. | Passwords are retained only for as long as required to allow access with access restricted to the Chief Officer and RFO to reduce the risk of unauthorised breaches and or financial losses. |
| Officers Work Mobile Phones - Limited work-related contact information and communications necessary for carrying out Council duties. Including WhatsApp group for lone working and quick communication of PGCC/HTC issues | Council-issued work mobile phones held by officers and facilities staff for PGCC related contact. | Whilst officer is in post. Any phones issued will be returned and re-configured before re-issuing | Yes | Council issued mobile phones are provided to enable officers to carry out their duties, including responding to operational issues and out of hours matters where necessary. Officers are instructed that NO Council or work-related information is to be stored on personal mobile phones. Work information is held only on Council-issued devices to maintain data | All data removed and device wiped when employment ends or when the device is replaced | Use of Council issued devices only supports data protection, security and accountability by ensuring work data is controlled, removable and protected against unauthorised access. |
| Officers work contact details (partners, community Groups and Individuals | Scribe CRM, Officers mobiles, Council e-mails | Whilst contact is active and as required for Council business | Yes | Officers are instructed that no Council or work related information is to be stored on personal mobile phones. Work information is held only on Council issued devices to maintain data security and separation between personal and work data. | Deleted when contact is no longer required or upon request | Retention is limited to what is necessary to support Council functions. Regular review ensures outdated or unnecessary contact details are removed to comply with data minimisation principles. |