COMPANY NAME:

Hillcrest

POLICY NUMBER:

HR 33

POLICY TITLE:

Personnel Files Policy

This document can be produced in different formats, for example, in larger print or audio-format, and in other languages, as appropriate. We promote equality through seeking to eliminate unlawful and unfair treatment on the ground of any protected characteristic, as appropriate.

## Policy: Underpinning and Supporting Documents

This policy should be read in conjunction with the following documents:

**Other Policies*:***

- G10 Data Protection Policy
- G18 Records Management Policy

**Compliance*:***

**Legislation*:***

- Data Protection Act 2018
- UK General Data Protection Regulation
- Privacy and Electronic Communications Regulations (PECR) and Data (Use and Access) Act 2025

**Best Practice:**

- CIPD
- ACAS

Hillcrest

## 1. Policy Statement

The purpose of this policy is to outline the conditions under which employee's personnel files are held, what information will be held, who maintains the files and the process for accessing the information contained within them. It also sets out the organisations approach to providing selected personnel information to employees via our Employee Self Service area (ESS).

By storing relevant and accurate information, it is the intention of the organisation to help speed up the provision of information and help the organisation with processes such as Recruitment and Selection, Absence Management, Workforce Planning and Training and Development.

Hillcrest is committed to storing useful and relevant information only, in accordance with the relevant Data Protection legislation.

## 2. Policy: Principles

- The Policy and Procedure will apply to all employees and relief workers working for Hillcrest.
- This policy also applies separately to any managers, or HR and Payroll staff who are involved in maintaining or accessing personal data
- The attached procedure provides guidance to employees on what steps they are required to take to access information held in their personnel file.
- All information stored will be in accordance with the relevant Data Protection legislation
- All information accessed will be used for appropriate purposes.
- The Data Protection Policy adds supplementary information relevant to this Policy.

Policy Definitions

- Electronic Personnel Files: Any digital record relating to an employees employment including Document Management system (or DM5) and iTrent.
- Employee Self Service (ESS): A secure digital platform that allows employees to view selected personnel documents
- Personal Data: Information relating to an identified, or identifiable individual
- Special category data: this includes any data with reveals someone's racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership. It also includes genetic data, biometric data when used to uniquely identify an individual (for example, facial recognition and fingerprint scanning), health data or data relating to someone's sex life or their sexual orientation.

## 3. Policy: Responsibilities

The HR Department

- Ensure that each Hillcrest employee and relief worker has their own electronic personnel file
- Be responsible for maintaining all personnel files and ensuring only information which is relevant and accurate is held
- Ensure that access to Personnel files and information is restricted to authorised individuals only
- Will determine which documents are suitable for visibility on Employee Self Service and Manager Self Service
- Only share information from the personnel file where appropriate and in line with the relevant Data Protection legislation
- Be responsible for ensuring information is destroyed in accordance with the organisations Records Retention Schedule including any personal data or documents recorded on our electronic HR Database (iTrent) and Document Management System (DM5)
- Assist the Business Services Team with any subject access requests for personnel files

Managers

- Provide documentation to HR promptly and securely
- Ensure any information forwarded to the HR team for keeping in employees personnel files is relevant and accurate
- Maintain confidentiality when handling employee information
- Will not hold personnel information in the establishment that is not relevant to hold

IT Department

- Responsible for maintaining the security of the electronic storage systems, ensuring that appropriate encryption, access control and back up measures are in place
- IT will ensure that all backups containing personnel file data are managed in accordance with the Records Retention Schedule and securely purged at the end of the retention period to prevent reconstruction or unauthorised access.
- IT will maintain and regularly test disaster recovery processes to ensure personnel file data can be restored promptly and securely in the even of the system failure or data loss

- IT will periodically review access permissions to ensure compliance with least privileges principles.

Business Services Team

- Will process and notify the HR team of any subject access requests to the personnel file

Policy Document Governance and Management

| | | |
|---|---|---|
| Author/ Lead: | Claire Balneaves, HR & Payroll Data & Systems Partner | |
| Version number: | V3 | |
| Current version referred for approval to: | A&GP | |
| Current version approved: | 24/02/2026 | |
| Date of next review: | 24/02/2031 | |
| Date of Equality Impact Assessment | 29/01/2026 | |
| Date of Privacy Impact Assessment: | Click here to enter a date. | N/A ☒ |
| Date of Environmental Impact Assessment: | Click here to enter a date. | N/A ☒ |

## Procedure Contents

COMPANY NAME:

Hillcrest

PROCEDURE NUMBER:

HR 33

PROCEDURE TITLE:

Personnel Files Procedure

This document can be produced in different formats, for example, in larger print or audio-format, and in other languages, as appropriate. We promote equality through seeking to eliminate unlawful and unfair forms of discrimination, as appropriate.

## 1. Introduction

This procedure aims to inform employees of how information contained in their personnel file will be held and processed within the organisation. This procedure should be read alongside the HR 33 Personnel Files Policy and the Records Management Policy

## 2. Storage of Personnel Files

All personnel files will be created and held in electronic format by the Human Resources Department in accordance with the Records Management Policy. No paper based information will be held. Any original medical certificates submitted to the HR Department will be returned to individual employees after a copy has been taken for the file.

The HR Department will be responsible for all personnel files and as such, will ensure all maintenance and appropriate access of files is strictly adhered to. Only accurate and relevant information will be held.

Disciplinary Warnings will no longer be classed as live warnings when they have reached the expiry date.

The HR Department will be responsible for deleting/destroying any information that is no longer required. This will be carried out in accordance with Hillcrest's Records Management Policy and Records Retention Schedules.

The HR Department will be responsible for ensuring only mandatory information is held following the exit of any employee from the organisation.

## 3. Mandatory Contents of Personnel Files

The HR Department have identified the following information as mandatory to be held within the Personnel file:-

- Application Form
- CV (where applicable)
- References
- Interview Assessment Sheet
- Offer of employment letter
- Withdrawal of offer letter (where applicable)
- Contract of Employment (signed)
- Contract Amendments (if applicable)
- Task Role Analysis
- Pre Employment Assessment Review from Occupational Health (where applicable)
- Right to Work checks (including Home Office report where applicable)
- Qualifications (if applicable)
- Disclosure Scotland – Self declaration

- Copies of ID for confirming the Right to Work in UK
- Probationary Review Forms
- Annual Review/EPDR Form and 6 monthly reviews
- Copy of any live Disciplinary Warnings
- Copies of any Risk Assessments
- Accident Records
- Resignation Letter
- Leaving Form

It is acknowledged that there will be other supplementary information that will in some circumstances be held on file however, this does not constitute mandatory information.

## 4. Accessing your Personnel File

### 4.1 Employee Self Service (ESS)

The organisation provides employees with access to selected documents from their Electronic Personnel File via the Employee self-service platform (ESS). This feature supports transparency and allows employees to view or download approved documents.

The following categories of documents may be visible, subject to system functionality and organisational approval:-

- Recruitment- such as application forms, identification, role profiles and offer letters
- Absence – such as medical certificates, appointment letters, sick pay entitlement letters and return to work forms
- Benefits – such as cycle to work or tech scheme agreements or Death in Service nomination forms
- HR Contractual – including a contract of employment, contract amendments, flexible working requests and outcomes and Change forms
- Training and Development – Annual Reviews, qualifications or certificates and copies of Funding Repayment agreements

Documents uploaded from 1 March 2026 onwards will be available for employees to view in ESS. Documents uploaded prior to this date will still form part of an employees personnel file but will not appear in ESS.

The following categories of documents will not be visible in ESS due to system limitations or their sensitive nature:

- Probationary review forms

- Medical records – such as Occupational health referrals and Occupational health reports
- Disciplinary invites and outcomes
- Grievance documentation
- Performance management information

These records will remain part of an employee personnel file and may be accessed via a formal subject access request.

Employees are not permitted to delete anything from their personnel file via employee self service. Where employees find information to be incorrect or out of date they must raise this via the HR Admin Team as soon as possible. Permission will be sought from the relevant HR Business Partner or HR & Payroll Data Systems Partner to either remove or update, as appropriate.

### 4.2 Subject Access Requests

Employees will have the right to request access to any information held within their HR Personnel file.

Employees can make a "Subject Access Request" to obtain access to their personnel file. All requests should be submitted in writing to the Business Services Team using informationgovernance@hillcrest.org.uk

Access to an employees file should only be permitted to the actual employee. Should Manager's request information relating to an employee, clarity will be sought as to whether this information is relevant and appropriate for sharing and what the purpose of the request is. In certain circumstances, authorisation may be sought from the employee concerned. Information will only be released to external parties when a signed letter of authorisation from the employee is presented with the request. Examples of situations such as this are when employment verification is required to support applications such as mortgage requests and credit applications.

## 5. Exceptions to this process

There are exceptions to the above process where information is requested by the HMI of taxes, a Court, the Police or other Public Body who has a legal right to access information held about you.

## 6. The Retention and Disposal of Personnel Files

When an employee leaves the organisation, their personnel file, including employment contracts, performance records, payroll information, any disciplinary documentation and training records, will be retained for a specified period in accordance with legal, regulatory and organisational requirements. This is documented in the organisations Records Retention Schedules.

Personnel files for former employees will normally be retained for 6 years from the employees last day of employment. Certain records may be retained for longer where legally required.

Electronic records will be protected through appropriate security controls.

At the end of the retention period, all records will be disposed of in a secure and confidential manner. Electronic records will be permanently deleted from all systems and back up environments, ensuring they cannot be reconstructed or accessed. IT will confirm that deletion of electronic records includes removal from all live systems and back up environments, ensuring irrecoverable

Procedure Document Governance and Management

| | |
|---|---|
| Author/ Lead: | Claire Balneaves, HR & Payroll Data & Systems Partner |
| Version number: | V3 |
| Current version referred for approval to: | Novella Tragham, Head of HR & OD |
| Current version approved on: | 24/02/2026 |
| Date of next review: | 24/02/2031 |
| Date of Impact Assessment: | 29/01/2026 |
| Date of Privacy Impact Assessment: | Click here to enter a date. N/A ☒ |
| Date of Environmental Impact Assessment: | Click here to enter a date. N/A ☒ |