Retention and Disposal Policy

REVIEWED: December 2025

NEXT REVIEW DATE: December 2026

REVIEWED BY: Olivia Bakewell

Introduction

The purpose of this policy is to detail the procedures for the retention and disposal of information to ensure that we carry this out consistently and that it is documented.

Registration and Retention of Candidate Information

When we register a candidate, their information is held in a number of places, on our software system and in Smile employee's emails (e.g. if they have emailed CVs or we have received references). Candidates registered between 2nd September 2019 – 1st September 2020 will have their information stored on People Compliance, an online cloud where documents can be securely uploaded and stored. If a candidate registered before September 2019, they will have a physical candidate folder which are kept in lockable filing cabinet, which we are in the process of moving online to our secure CRM. The system records are held on our CRM and People Compliance are accessible to users only by a password. Emails are accessible to Smile employees remotely and on their phones- however this access is also password protected. Overnight in the office computers are either turned off or locked to prevent access and confidential information is put away each night in lockable cupboards.

Archiving Of Candidate Information

When a candidate no longer requires work through us we archive a folder. The process for this is that we change the status of the candidate file on the system to archived so they are not regularly contacted. A note is logged on the contact log as to why the folder has been archived, the archive date is written on the physical folder, any DBS copies are removed from the candidate folder and placed in a separate folder, any copies of the DBS held on our system are also moved into a separate folder and the physical folder is placed into our lockable archive cabinet as DBS copies are only held for 6 months after the last recruitment decision.

For candidates on CRM, the process is the same and after 2 years from their last assignment date, the majority of their personal data and documents will have been removed. We must retain specific data under Conduct of Employment Agencies and Employment Businesses Regulations 2003 and safeguarding guidelines for all candidates who have been cleared for work for 7 years from their last assignment.

This includes:

- Name/Address
- Terms of Engagement
- Booking Confirmations and Booking History with school names/dates
- Qualifications and Training for the role they have completed
- Any causes for concern/allegation record during this time (to be held securely by DPO)

Reviewing Of Candidate Information

The compliance team checks the folders holding the candidate's DBS information both on the system and in the cupboard monthly and deletes/places in the shredding box the DBS after 6 months of the candidate being archived.

Weekly, the compliance team go through the cabinets removing candidate folders that were archived over a year ago (checking this by the archive date written on the folder and double checking the archive date logged on our system) and scanning in the contents of their folder to be held on our system for further year.

Stopping Contact with Candidates

After the two-year retention period of candidate information, we remove document copies and completed forms, references etc. After this stage, the candidate's documents are no longer accessible online. As mentioned above in point 3, we retain certain information for safeguarding reasons. The records retained are listed above.

If a candidate asks to not be contacted and their information to be removed, we delete their contact details, CV and any identifiable information from their candidate record we hold on the system.

On all emails we send we have the line 'If you want to opt out from receiving marketing emails from us please email admin@smile-education.co.uk with the subject title MARKETING OPT OUT'. This email is checked daily and requests acted upon quickly. We then untick their GDPR preferences for marketing, which is time and date stamped. This blocks any marketing material from being sent to that candidate. However, we still hold the physical copy of their information for the two years required by Compliance Plus for safeguarding reasons.

Other Information Held

We also hold a variety of other information which we keep secure. Client information is held on our system on MatchMaker which can only be accessed by individuals working for Smile Education by logging onto their computers and then logging into the system with a password.

Internal Payroll and HR documents for Smile Employees are held in an HR drive only accessible by the Directors and HR manager additionally in physical folders which are kept securely. We have an old database

system (RDB) that is no longer in use for contacting clients and candidates but continues to be used for providing work dates and is accessible only on one secure drive with limited access.

Allegations

In the case of an allegation made against a candidate, the DSL or Deputy DSL should keep a clear and comprehensive record of the allegation, decisions reached, and actions taken on the person's personnel file, a copy of which should be given to them.

The record should include details of how the allegation was followed up and resolved, the decisions reached, and the action taken. It should be kept at least until the person reaches normal retirement age or for 10 years if longer.

The record will provide accurate information for any future reference and provide clarification if a future DBS disclosure reveals an allegation that did not result in a prosecution or a conviction. It will prevent unnecessary re-investigation if allegations should resurface.

Details of allegations that are found to be malicious should be removed from personnel records.

Each agency/organisation must take great care to ensure that the records they keep respect the confidentiality of the alleged victim and/or the accused adult. **This information will be held in a secure drive only accessed by the DSL, or Deputy DSL.**