



Subject Access Request Policy

Purpose and Scope

VES Recruitment (VES) respects the right of individuals to access their personal data under the UK GDPR and Data Protection Act 2018. This policy explains how we recognise, record and respond to subject access requests (SARs) from candidates, temporary workers, employees, former workers, clients and other individuals whose personal data we hold.

A SAR concerns the requester's **own personal data**. It is not automatically a right to every document in a file or to another person's information. We will identify and disclose relevant personal data, together with the supplementary information required by law, subject to any applicable exemption.

Making a request

An individual may make a SAR verbally or in writing, including by email, letter, telephone or social media. They do not need to use the words “subject access request”, give a reason or complete a particular form. Requests can be made to any VES team member.

Requests may be sent to mollyelliott@vesrecruitment.co.uk or **Suite 2, The Business Centre, Pentrebach, Merthyr Tydfil, CF48 4TQ**. Staff receiving a request elsewhere must forward it promptly to the Data Protection Lead, recording the date received and the requester's exact words. Staff must not promise disclosure or decide for themselves that a request is invalid.

Someone acting on another person's behalf must provide evidence of their authority. Requests concerning a child require careful assessment of the child's ability to exercise their own rights, any parental responsibility and the child's best interests.

Responsibility

The Data Protection Lead coordinates each SAR, maintains the request log, sets the deadline, directs searches, reviews possible exemptions, approves the response and arranges secure delivery. Relevant managers and system owners must promptly search the locations they control and preserve relevant information.

Any potential safeguarding, confidentiality or legal issue must be referred to the Data Protection Lead before disclosure. Where appropriate, the Lead will obtain specialist legal advice.

Timescales

We will respond without undue delay and normally within **one calendar month** of receiving the request. If we reasonably need to confirm identity or a representative's authority, we will ask promptly; the response period begins when the required evidence is received.



If a request is complex or the individual has made a number of requests, we may extend the deadline by up to **two further months** where necessary. We will tell the requester within the original one-month period and explain the reason.

We may seek clarification only where reasonably necessary to respond effectively. Where the legal conditions for clarification are met, the response clock pauses while we await it. We will continue to deal with information we can reasonably provide without clarification.

Identify checks and acknowledgement

We will verify identity proportionately, using information already held where appropriate. We will request formal ID only when needed and use a secure method to receive it. We will acknowledge the request, confirm any information needed to locate records, and explain the expected response date. A complaint, dispute or concern about a decision does not remove the right of access.

Locating Information

We will conduct reasonable and proportionate searches of relevant systems and records. Depending on the request, these may include Bullhorn, Kyloe Connect, Colleago, payroll and Sage records, recruitment and compliance records, references, booking records, email, messages, shared files and relevant paper records.

The search must cover personal data held at the time of the request, including relevant opinions or decisions about the individual where recorded. Staff must preserve relevant records and follow normal retention rules; they must not delete, amend or conceal information because a SAR has been received. We will document the systems searched, search terms, custodians, date ranges and any limits applied.

Reviewing and Disclosing Data

The Data Protection Lead will review material for relevance, accuracy of attribution, third-party information and applicable exemptions. Information about pupils, residents, patients, referees, colleagues, clients or safeguarding reporters requires particular care. We will consider redaction, consent and whether disclosure without consent would be reasonable; we will not automatically withhold an entire document simply because it mentions another person.

Any exemption, including one relating to confidential references, legal privilege, safeguarding or the rights of others, will be assessed case by case and documented. The fact that a reference is sensitive or marked confidential does not by itself decide whether it can be withheld. If we withhold data, we will explain our decision to the extent permitted by law.

We will provide a copy of the individual's personal data and the required supplementary information, including relevant purposes, categories, recipients, retention information, sources where available, rights and complaint routes. We will use clear language and an accessible, commonly used format. Electronic requests will normally receive an electronic response unless another format is requested.



Before sending, a second authorised person will check the recipient, attachments, redactions and delivery method. Sensitive material will be shared securely.

Fees and Refusals

SARs are normally free. We may charge a reasonable administrative fee for additional copies or where a request is manifestly unfounded or excessive, where the law permits. We may refuse a manifestly unfounded or excessive request only after an individual, documented assessment. We will inform the requester of any refusal, reasons where possible, and their right to complain to the Information Commissioner's Office (ICO) and seek a judicial remedy.

Records and Reviews

We will retain a secure SAR log recording receipt, identity checks, deadline changes, searches, decisions, exemptions, response date and delivery method. Records relating to a SAR will be retained according to VES's retention schedule. The Data Protection Lead will review this policy at least annually and when relevant law or ICO guidance changes.

Related documents: Privacy notice; data retention policy; information security policy; safeguarding policies; complaints procedure.

ICO: <https://ico.org.uk/make-a-complaint/>