CANDIDATE PRIVACY POLICY

This policy was reviewed on:

Date: 23rd September 2026

By: Louis Mapp

Approved by: Senior Management Team

Policy will be reviewed on: 23rd September 2027

Frequency of review: Every 1 year(s) or sooner if government legislation or regulatory guidance changes

Data Protection Officer: Louis Mapp - louis@1ststaff.co.uk

1 Purpose and Status of this Document

This Candidate Privacy Policy explains how 1st Staff Limited ("1st Staff", "we", "our" or "us") collects, uses, stores, shares and protects Personal Data relating to people who apply to work with us, are identified as potential candidates, are referred to us, or progress through our recruitment and onboarding process.

For the purposes of UK data-protection law, this document also serves as the **Candidate Privacy Notice** required by Articles 13 and 14 of the UK General Data Protection Regulation (UK GDPR).

1st Staff Limited is the **Data Controller** for the candidate recruitment information covered by this document. We determine why and how this information is processed for our own recruitment, safer-recruitment, workforce planning and onboarding purposes.

This document is intended to provide transparent information throughout the candidate journey. It does not create a right to employment, work, hours, a placement or a particular start date.

2 Legal and Regulatory Framework

Candidate information is processed in accordance with applicable law and regulatory guidance, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Privacy and Electronic Communications Regulations 2003 (PECR), where applicable to recruitment communications;
- Equality Act 2010;
- Safeguarding Vulnerable Groups Act 2006;
- Protection of Freedoms Act 2012;
- Rehabilitation of Offenders Act 1974 and applicable exceptions, as amended;
- Education Act 2002;
- Keeping Children Safe in Education (KCSIE) 2026;
- Working Together to Safeguard Children; and
- relevant Information Commissioner's Office (ICO), Disclosure and Barring Service (DBS), Home Office and Department for Education guidance.

3 Related 1st Staff Policies and Procedures

This policy should be read alongside the following 1st Staff policies, notices and procedures where relevant:

- Data Protection Policy;
- Safe Recruitment Policy;
- Staff/Workers Privacy Notice;
- Child Protection & Safeguarding Policy;
- Managing Allegations Against Staff, Volunteers & Low-Level Concerns Policy;
- Staff Code of Conduct;
- Online Safety & IT Use / E-Safety Policy;
- Information Security Policy;
- Records Management & Retention Schedule Policy;
- Data Breach Procedure;
- Subject Access Request Procedure;
- Whistleblowing Policy;
- Induction, Training, Supervision and Support Policy;
- Complaints Policy; and
- the approved Recruitment and Interview Process / workflow.

Where one of these documents sets a specific operational requirement, that requirement applies together with the privacy controls in this document. If there is uncertainty about how candidate information should be handled, the Data Protection Officer should be consulted.

4 Who We Are and How to Contact Us

Controller: 1st Staff Limited

Operational address: The Civic Building, 2nd Floor, 323 High Street, Epping, CM16 4BZ, United Kingdom

Data Protection Officer: Louis Mapp

Email: louis@1ststaff.co.uk

Questions about this policy, the processing of candidate information or the exercise of data-protection rights should be directed to the Data Protection Officer.

5 Definitions

Candidate

A person who has applied to work with 1st Staff, has been identified through a recruitment or talent-search process, has been referred to us, or is being considered for future work.

Recruitment Database

The approved system used to hold prospect and candidate information while the person is progressing through recruitment. Candidate progression outcomes in this database include **Suitable to Progress**, **Not Suitable to Progress, or Registered but not currently progressing**. Active/Inactive staff status is not used as the candidate recruitment outcome.

Staff Database

The approved workforce record used after the individual reaches the formal staff/onboarding threshold. Staff records may then be marked **Active** or **Inactive** according to workforce status. Entry into the Staff Database does not by itself authorise deployment to a pupil.

Tutor Pool

A controlled matching status, view or pool within the authorised workforce system for people who have reached the relevant recruitment/induction stage and may be considered by Area Leads for suitable work. It is not an uncontrolled duplicate candidate database.

Personal Data

Information relating to an identified or identifiable living individual. This includes factual information and recorded opinions or professional assessments about that individual.

Special Category Data

Personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, health information, sex life or sexual orientation.

Criminal Offence Data

Personal information relating to criminal convictions, offences, allegations, cautions, proceedings, DBS information, barred-list information or related criminal-record matters.

Processing

Any operation performed on Personal Data, including collecting, recording, organising, storing, viewing, using, analysing, sharing, correcting, transferring, deleting or destroying it.

Controller

An organisation that determines the purposes and essential means of Processing Personal Data.

Processor

An organisation that Processes Personal Data on documented instructions from a Controller.

6 How We Obtain Candidate Information

We may obtain candidate information from:

- you directly, including through an advert, application form, CV, screening call, Registration Pack, interview, email, telephone or other recruitment interaction;
- job-board CV databases where your settings or the service make your profile available to recruiters;
- professional networking platforms and other public professional sources where recruitment contact is reasonably expected;
- careers fairs, recruitment events, exhibitions or other events where you provide details;
- a current or former 1st Staff tutor, employee or other person who refers you;
- referees, current or former employers, educational institutions or professional bodies, where appropriate;
- official or authorised checking services used for identity, right-to-work, qualifications, teaching restrictions, safeguarding or criminal-record checks;
- publicly available information used for proportionate safer-recruitment online due diligence, where applicable; and
- information already lawfully held by 1st Staff from a previous application, engagement or working relationship where it remains appropriate and lawful to use it for recruitment.

Where we obtain your information from another source, we will provide the required privacy information within the period required by law and, where practicable, at or before our first substantive contact with you. We will explain the source or category of source where required.

7 What Candidate Information We Collect

The information collected depends on the stage you reach. We apply data minimisation so that information is collected only when it is reasonably needed for the current stage.

7.1 Prospect and Screening Stage

At the earliest stage we may collect:

- full name;
- telephone number;
- personal email address;
- broad geographical location where needed to identify the relevant recruitment area and travel feasibility;
- current or recent role and relevant experience;
- teaching, tutoring, SEND/SEMH, behaviour, mentoring or Alternative Provision experience where relevant;
- subjects, key stages, phases and qualifications at a high level;
- availability and preferred delivery settings;
- source of the candidate record;
- screening notes and screening outcome; and
- callback or future-contact preference.

A full residential address, full address history, identity evidence, detailed health information or criminal-record information should not ordinarily be collected during the initial screening conversation unless there is a specific lawful and operational reason.

7.2 Formal Application and Registration Stage

Candidates progressing beyond initial screening will normally be asked to provide both the **1st Staff application form and a current CV**. Additional Registration Pack information may include (**Registration does not require the candidate to have uploaded all supporting evidence. Where supporting documents are not immediately available, the candidate may still complete and submit their Registration Pack and remain registered with 1st Staff. Outstanding evidence becomes mandatory only when the candidate chooses to progress to the relevant recruitment stage**):

- full legal name and previous names where required;
- full address and address history where required for compliance;
- date of birth where required for identity or statutory checks;
- full employment history and reasons for leaving;
- explanations for gaps in employment;
- education, qualifications and professional status;
- professional references and referee details (minimum **two referee details at Registration**, candidate chooses which may be contacted immediately; **one satisfactory reference before Interview**, remaining/core reference before deployment);

- right-to-work and identity information;
- travel, driving and deployment preferences;
- availability and role preferences; and
- information necessary to administer reasonable adjustments or the recruitment process lawfully.

Compliance gates:

- **Before Interview:** identity evidence, proof of address and at least one satisfactory reference.
- **Offer:** conditional upon DBS clearance, and positive reference outcome (2 mandatory references) at the time of deployment.
- **Before Deployment:** all mandatory training and induction, remaining required/core reference, DBS clearance, Lone Worker Risk Assessment and any other final safer-recruitment or compliance requirements.

7.3 Interview and Assessment Stage

- interview date and panel membership;
- responses to professional and role-specific questions;
- responses to safeguarding and safer-recruitment questions;
- scoring and structured assessment;
- employment-history and gap explanations;
- relevant online-search points requiring clarification;
- panel notes, rationale and decision;
- any development or training needs identified; and
- recording/transcription information where an approved tool is used.

7.4 Compliance and Vetting Stage

- identity verification;
- right-to-work evidence and check status;
- references and reference verification;
- qualification evidence and professional-status checks;
- enhanced DBS and barred-list check status where applicable;
- prohibition or restriction checks where applicable;
- overseas criminal-record or professional checks where appropriate;
- E-Safety / Online Safety acknowledgement where required by the recruitment process; and
- other lawful safer-recruitment checks required for the role.

8 Health, Disability and Equality Information

1st Staff will not routinely ask candidates detailed questions about health or disability before a job offer or placement in a pool of successful candidates, except where the Equality Act 2010 permits those questions.

Before that stage, health or disability information may be requested only where necessary for purposes such as:

- identifying reasonable adjustments needed for an interview, assessment or recruitment process;
- establishing whether a candidate can carry out a function that is intrinsic to the role, taking reasonable adjustments into account;
- lawful positive action; or
- equality monitoring, which should be separated from selection information and restricted from decision-makers wherever practicable.

Where fuller health information is lawfully required after a conditional offer or at a later onboarding stage, it will be restricted to authorised personnel and will not be made available to interview panel members unless there is a specific lawful need.

Information supplied solely to arrange a reasonable adjustment must not be used to disadvantage a candidate in the capability decision.

9 Why We Use Candidate Information and Our Lawful Bases

We process candidate information only where an appropriate lawful basis applies. More than one basis may apply to the recruitment journey.

9.1 Legitimate Interests

We have legitimate interests in identifying and maintaining a suitable supply of tutors, teachers and other staff; responding to referral demand; managing recruitment activity; maintaining accurate recruitment records; preventing duplicate or fraudulent applications; quality assurance; audit; security; and establishing, exercising or defending legal claims. We assess those interests against the rights and reasonable expectations of candidates.

9.2 Steps Before Entering into a Contract

Where you choose to progress and ask us to consider you for work, we may process information where necessary to take steps at your request before entering into a contract, including registration, assessment, interview, offer and onboarding activity.

9.3 Legal Obligations

We process information where necessary to comply with applicable legal and regulatory obligations, including right-to-work requirements, safeguarding and safer-recruitment duties, employment-law requirements and statutory record-keeping.

9.4 Consent

We do not normally rely on consent for core recruitment processing where another lawful basis is more appropriate. Where we specifically rely on consent for an optional activity, you may withdraw that consent at any time without affecting Processing already carried out lawfully.

9.5 Legal Claims and Regulatory Matters

Relevant recruitment information may be used or retained where necessary to establish, exercise or defend legal claims, respond to complaints, cooperate with lawful investigations or meet regulatory requirements.

10 Special Category Data and Criminal Offence Data

Special Category Data and Criminal Offence Data receive additional protection and are processed only where the relevant conditions in the UK GDPR and Data Protection Act 2018 are met.

Depending on the circumstances, lawful conditions may include employment and social-protection obligations, substantial public interest grounds, safeguarding, equality monitoring, legal claims or vital interests. Criminal Offence Data is processed only where authorised by law and an applicable Schedule 1 condition is met, with an Appropriate Policy Document maintained where required.

Recruiters and interview panels do not receive unrestricted access to health declarations, DBS certificate content, conviction details or other restricted Compliance information. They should normally receive only the status or conclusion necessary for their role, such as **complete, in progress, clarification required or not cleared**.

11 Recruitment Sourcing, Direct Contact and Objections

1st Staff may identify potential candidates through job boards, recruitment databases, professional networks, referrals and other lawful recruitment channels.

Where we proactively contact a person who has not applied directly, we will consider whether recruitment contact is reasonably expected in the context of the source and whether our legitimate interests are balanced against the individual's rights. Electronic recruitment communications will also comply with PECR where those rules apply.

We will not use intrusive methods to obtain private information or deliberately bypass privacy settings in order to source candidates.

If you tell us that you do not wish to receive further recruitment contact, we will stop the relevant contact and may retain only the minimum suppression information necessary to ensure that your preference is respected.

12 Recruitment Database, Screening and Application Records

Candidate information is held in the approved **Recruitment Database** while the individual is progressing through recruitment. Access is role-based and recorded where the system supports audit logging.

The Recruitment Team performs the first-stage screening. This may include review of the application/CV and, where appropriate, a telephone call, online meeting or face-to-face meeting.

For workflow purposes, the Recruitment Team records the candidate as:

- **Suitable to Progress** - the candidate may proceed to the next recruitment stage; or
- **Not Suitable to Progress** - the candidate does not progress in that recruitment exercise.
- **Registered but not currently progressing** - candidate has completed registration and may remain within the Recruitment Database for future opportunities but is not currently progressing through the compliance/recruitment stages.

The reason for a recruitment decision must be factual, relevant, proportionate and professionally worded. Notes must distinguish objective facts from professional judgement and must not contain irrelevant comments about protected characteristics or other private matters.

Where the application form, CV or other recruitment information contains inconsistencies, unexplained gaps or material discrepancies, these may be recorded and explored in accordance with the Safe Recruitment Policy.

13 Shortlisting and Online Due-Diligence Searches

Shortlisting, online due diligence and safer-recruitment checks are governed by the Safe Recruitment Policy. Candidate information used for these purposes must also comply with this privacy policy.

Where an online search is undertaken as part of safer-recruitment due diligence:

- candidates will be informed that such a search may be undertaken;
- the search must have a defined safer-recruitment or suitability purpose and be proportionate to the role;
- only publicly available information should ordinarily be used;
- staff must not use deceptive accounts, bypass privacy controls or seek irrelevant private material;
- the person carrying out the search should, wherever practicable, screen out irrelevant information before findings are provided to decision-makers;
- protected characteristics and irrelevant personal information must not influence the selection decision;
- only relevant findings should be retained in the candidate record;
- information found online must not be assumed to be accurate merely because it is public; and
- where a potentially adverse finding may influence a decision, the candidate should normally have an opportunity to explain or correct the information before a final decision is taken.

Whole-page screenshots, browsing histories or irrelevant social-media content should not be retained where a short factual record of the relevant finding is sufficient.

14 Interview Process and Panel Access

Formal interviews are conducted in accordance with the Safe Recruitment Policy and the approved Interview Process. The panel must receive only the information necessary to assess professional capability, role suitability and safeguarding suitability.

The interview panel structure is determined by the Safe Recruitment Policy. Under the current 1st Staff model, the panel contains at least two staff members and collectively includes the required safer-recruitment trained member, and the Area Lead or an independent assessor with safer-recruitment training; one person may satisfy more than one of those role requirements.

Panel members may normally access information including:

- candidate name and role applied for;
- application form, CV or relevant professional profile;
- teaching/subject profile and qualifications relevant to the role;
- relevant SEND, SEMH, behaviour, mentoring, school or Alternative Provision experience;
- availability and relevant geography;
- employment history and gap explanations;
- safeguarding responses and interview assessment information;
- IT capability where relevant; and
- high-level Compliance status where needed.

Panel members do not ordinarily require access to full date-of-birth evidence, nationality/immigration documents, full address history, National Insurance number, emergency contacts, detailed health information, full DBS/conviction content, referee contact details or irrelevant source/referral information.

15 Screening Calls, Interview Recordings, Transcripts and AI

Screening calls and interviews may be transcribed or recorded only through an approved organisational system and for a defined recruitment, safer-recruitment, quality, audit or evidential purpose.

Where recording or transcription is used:

- the candidate will be given clear notice;
- the system and provider must be approved under 1st Staff data-protection and information-security arrangements;
- access must be limited to authorised staff;
- the transcript or summary should be reviewed by a human before it becomes part of the formal recruitment record;
- material inaccuracies should be corrected or annotated;
- AI-generated summaries are administrative aids and must not be treated as an infallible account; and
- 1st Staff will not make a significant recruitment decision solely by automated means without the safeguards required by law.

Routine long-term retention of full audio or video recordings is not necessary merely because a transcript exists. Unless there is a documented reason to retain the recording,

such as an active complaint, investigation, legal claim or quality review, the underlying recording should be deleted once the required formal record has been verified.

Personal or confidential candidate information must not be copied into publicly available AI tools or unapproved transcription services.

16 Compliance, References and Vetting Information

Compliance activity is managed by authorised personnel under the Safe Recruitment Policy. Depending on the role and recruitment stage, this may include identity, right-to-work, qualifications, references, DBS/barred-list information, teaching restrictions, overseas checks and other lawful suitability checks.

16.1 References

References are confidential recruitment information. We may contact referees, previous employers or professional bodies to verify information and assess suitability where lawful and appropriate. Any material discrepancy may be explored with the candidate. Referee information is restricted to staff who need it for recruitment, compliance or safeguarding purposes.

16.2 DBS and Criminal-Record Information

DBS certificate content and Criminal Offence Data are restricted to authorised Compliance, HR, Safeguarding or senior decision-makers as appropriate. The recruitment system should record only the minimum information necessary to evidence the check and decision. Copies of DBS certificates must not be retained for longer than necessary.

16.3 Safeguarding or Suitability Concerns

Where a serious safeguarding or professional-suitability concern arises during recruitment, information may be restricted and escalated to the Designated Safeguarding Lead or another authorised decision-maker. The matter will be handled in accordance with the Safe Recruitment, Child Protection & Safeguarding and Managing Allegations/Low-Level Concerns arrangements as applicable.

17 How Information Moves Through the Recruitment Journey

The operational sequence is governed by the Safe Recruitment Policy and approved workflow. For privacy and systems purposes, the normal data lifecycle is:

1. **Prospect / initial contact** - a limited candidate record is created and the source is recorded.
2. **Recruitment screening** - the Recruitment Team assesses whether the person is suitable to progress and records Suitable to Progress or Not Suitable to Progress.
3. **Application / registration** - the candidate provides the application form and CV and, where required, completes the secure Registration Pack.
4. **Compliance and safer-recruitment activity** - authorised staff undertake the checks appropriate to the stage. Some checks may begin before interview (**ID + proof of address + one satisfactory reference before Interview**) and outstanding checks may continue afterwards in accordance with the Safe Recruitment Policy.
5. **Formal interview** - the approved interview panel assesses professional and safeguarding suitability and records the formal panel outcome.
6. **Conditional approval / offer** - where the candidate passes interview, a conditional offer may be issued. The offer remains subject to satisfactory completion of all outstanding safer-recruitment and compliance checks before the individual is authorised to work.
7. **Staff Database transfer** - once the formal threshold set by the Safe Recruitment and onboarding process is met, only the information required for the continuing relationship transfers to the Staff Database. The staff record may then be Active or Inactive.
8. **Company account / system access** - Company email and other access are created only when authorised by the relevant onboarding/IT trigger and must follow least-privilege access controls.
9. **Induction and Tutor Pool** - after the required induction stage, the individual may become visible within the Tutor Pool or matching view for authorised Area Leads.
10. **Selection and deployment** - deployment to a pupil occurs only when all mandatory organisation-level and referral-specific requirements are complete (**EduCare courses, Induction, remaining/core reference, DBS clearance, Lone Worker Risk Assessment and any final compliance requirements**).

Information must not be duplicated indefinitely between the Recruitment Database and Staff Database. Once transferred, candidate-only information that no longer serves a lawful purpose should be deleted or archived in accordance with the Records Management & Retention Schedule.

Being recorded in the Staff Database, being marked Active, or appearing in the Tutor Pool does not by itself guarantee work or authorise a specific pupil deployment.

18 Role-Based Access and Internal Sharing

Candidate information is made available internally only on a need-to-know basis. Access should be configured according to role rather than general departmental visibility.

Role	Normal access position
Recruitment / Resourcer	Contact/source information, screening details, application/CV information and progression data needed to manage the candidate relationship. No routine access to detailed health, DBS/conviction content or other restricted Compliance data.
Compliance	Identity, right to work, references, qualifications, DBS and other vetting evidence necessary to determine clearance. Restricted information must remain within authorised Compliance access.
Interview Panel	Information necessary to assess capability and safeguarding suitability, including application/CV, relevant experience, work history/gaps, safeguarding responses and high-level Compliance status. No routine access to restricted sensitive evidence.
Safeguarding	Access only where a safeguarding, allegation, professional-suitability or safer-recruitment issue requires specialist consideration. No standing access beyond the safeguarding purpose.
HR / Onboarding	Offer, acceptance, contractual, personnel and onboarding information required once the candidate reaches the relevant stage. Recruitment information not needed for HR responsibilities remains restricted.
Area Leads	Relevant candidate/tutor profile information needed for matching, including capability, geography, availability and appropriate suitability status. Restricted Compliance content remains unavailable.
IT	Only the identity and onboarding/access information necessary to create, change or disable authorised Company accounts and systems.
Senior Management	Access only where needed for approval, governance, risk, legal, safeguarding or escalated recruitment decisions.
Bids / Referrals / Workforce Planning	At an approved future-supply stage, limited aggregated or profile information needed to understand resource capacity. Underlying sensitive recruitment and Compliance evidence is not provided unless specifically required and lawful.

19 External Sharing and Recipients

We may share candidate information externally only where there is a lawful, necessary and proportionate reason. Recipients may include:

- approved recruitment, applicant-tracking, HR, communications, e-signature and training providers;
- reference, identity, right-to-work, DBS, qualification or other authorised vetting service providers;
- referees, employers, educational institutions, awarding bodies or professional regulators where verification is required;
- government, safeguarding, law-enforcement, professional or regulatory bodies where disclosure is required or permitted by law;
- legal advisers, insurers, auditors and other professional advisers where necessary; and
- commissioners only where there is a specific lawful and operational reason, normally limited to assurance or deployment information rather than the underlying candidate file.

We do not sell candidate information. Candidate data is not disclosed to a commissioner merely because an individual has entered the recruitment pipeline or Tutor Pool.

20 Service Providers and International Transfers

Approved service providers may process candidate information on our behalf. Before use, 1st Staff will assess the provider, the information involved, contractual controls, security arrangements, sub-processing and retention.

Where Personal Data is transferred or made accessible outside the United Kingdom, 1st Staff will use a lawful transfer mechanism and appropriate safeguards, such as UK adequacy regulations, the UK International Data Transfer Agreement, an approved UK Addendum or another mechanism permitted by law.

The use of cloud, AI, transcription or recruitment technology does not remove 1st Staff's responsibility to assess where data is processed and whether international-transfer safeguards are required.

21 Security, Accuracy and Data Minimisation

1st Staff applies technical and organisational controls designed to protect candidate information from unauthorised access, loss, alteration or disclosure. Controls include role-

based access, secure organisational accounts, authentication controls, approved storage, audit logs where available and staff confidentiality obligations.

Recruitment records must be accurate, relevant and professional. Notes should distinguish:

- objective facts;
- information provided by the candidate;
- information received from a third party; and
- professional judgement or assessment.

Recruiters should redirect candidates away from disclosing unnecessary sensitive information during an initial screening call. Sensitive information required later must be collected through the approved secure process.

Candidate information must not be stored in personal email accounts, personal cloud storage, unauthorised messaging applications or unapproved AI systems.

22 How Long We Keep Candidate Information

We keep candidate information only for as long as it is needed for recruitment, safer recruitment, workforce planning, legal or regulatory obligations, safeguarding, complaints, investigations or legal claims. The normal periods are set out in Appendix 1 and must be read with the Records Management & Retention Schedule.

Retention periods are reviewed rather than treated as permission to keep information indefinitely. Where a candidate record remains in a future-contact or Tutor Pool status, the record must be reviewed periodically for accuracy, availability and continued relevance.

A legal hold, safeguarding matter, complaint, investigation or live claim may require information to be retained beyond the normal period. The reason for extended retention must be documented.

23 What Happens if You Do Not Provide Information

Some information is optional, while other information is necessary for us to consider you for work, complete safer-recruitment checks or meet legal obligations.

If you do not provide information that is necessary for a particular recruitment stage, 1st Staff may be unable to:

- assess your application;
- verify your identity or right to work;

- obtain or verify references;
- complete safeguarding or DBS checks;
- assess professional suitability;
- make or maintain a conditional offer;
- transfer your record into the Staff Database; or
- authorise you for deployment.

We will not require information that is not reasonably necessary for the recruitment or compliance purpose concerned.

24 Your Data Protection Rights

Depending on the circumstances and applicable legal exemptions, you may have the right to:

- request access to Personal Data we hold about you;
- ask us to correct inaccurate or incomplete information;
- ask us to erase information where there is no lawful reason to retain it;
- ask us to restrict Processing in certain circumstances;
- object to Processing based on legitimate interests, including proactive recruitment contact;
- receive certain information in a portable format where the right to data portability applies;
- withdraw consent where we rely on consent;
- request safeguards and meaningful human reconsideration in relation to qualifying significant automated decisions; and
- complain to 1st Staff and to the Information Commissioner.

Requests should be sent to the Data Protection Officer at louis@1ststaff.co.uk. We may need to verify your identity. We will respond within the timeframe required by data-protection law and will conduct reasonable and proportionate searches where applicable.

A request to correct information does not necessarily require us to replace a documented professional opinion with the candidate's preferred view. However, factual inaccuracies should be corrected and disputed professional assessments may be appropriately annotated where necessary.

25 Recruitment Contact, Future Contact and Suppression

You may ask us to stop recruitment contact at any time. We will record the appropriate outcome and stop contacting you through the relevant route.

If the timing is not right but you want to hear from us later, we may record an agreed future-contact date. We will keep only information reasonably needed for that purpose and will review the record in accordance with Appendix 1.

Where you object to future recruitment contact, we may retain a minimal suppression record for as long as reasonably necessary to prevent accidental re-contact. A suppression record is used to respect your objection, not to continue recruitment activity.

26 Data Protection Complaints

You have the right to complain directly to 1st Staff if you believe your Personal Data has been handled unlawfully or your data-protection rights have not been respected.

Complaints may be submitted electronically to the Data Protection Officer at louis@1ststaff.co.uk or through another accessible route provided by 1st Staff.

For complaints received on or after 19 June 2026, 1st Staff will comply with the statutory complaint-handling requirements introduced by the Data (Use and Access) Act 2025. This includes acknowledging the complaint within 30 days, taking appropriate steps to investigate and respond without undue delay, and keeping the complainant appropriately informed of progress.

You may also complain to the Information Commissioner's Office (ICO), the UK supervisory authority. Current contact details and guidance are available at ico.org.uk.

27 Personal Data Breaches

If candidate information is lost, disclosed to the wrong person, accessed without authority, corrupted, sent through an unapproved system or otherwise compromised, the incident must be handled under the 1st Staff Data Breach Procedure.

Where 1st Staff is the Controller, the Data Protection Officer will assess risk, document the decision and make any required notification to the ICO or affected individuals within the statutory requirements.

Candidates who become aware of a suspected breach involving their recruitment information should contact the Data Protection Officer as soon as possible.

28 Changes, Governance and Review

This policy is owned by the Data Protection Officer and approved by the Senior Management Team. It will be reviewed at least annually and sooner where there is a significant change to data-protection law, KCSIE, ICO guidance, the recruitment workflow, the Recruitment or Staff Database, AI/transcription technology, safer-recruitment requirements or the categories of candidate information processed.

The current version will be made available through the recruitment process and, where appropriate, on the 1st Staff website or candidate portal. The candidates must read/acknowledge the policy before completing the detailed Registration Pack.

Material changes that affect how candidate information is used will be communicated appropriately.

Appendix 1

Candidate Retention Schedule

Situation	Normal retention approach
Prospect contacted but did not proceed	Normally 6 months from the last meaningful contact, unless an objection or deletion request justifies earlier deletion or a lawful reason requires longer retention.
Asked us to contact them later	Up to 12 months from the last contact or agreed callback date, then review before any further retention or contact.
Applied / screened / interviewed and unsuccessful	Normally 6 months from notification of the recruitment outcome, unless a complaint, claim, safeguarding matter or legal obligation requires longer retention.
Registered but not currently progressing / did not complete clearance	Normally up to 12 months from the last meaningful recruitment activity, subject to earlier deletion where appropriate.
Approved / conditionally accepted and progressing	For the duration of the active recruitment/onboarding process, then transferred or retained under the applicable staff/personnel schedule.

Situation	Normal retention approach
Tutor Pool / matching status but no deployment	Retained only while the person remains genuinely available and relevant for matching. Availability and continued relevance must be reviewed at least every 12 months.
Candidate becomes staff / tutor / worker	Only relevant recruitment and verification information transfers to the Staff Database/personnel record. It is then retained under the Records Management & Retention Schedule.
Interview/screening transcript	Retained with the applicable recruitment record where it forms part of the formal evidence trail.
Underlying audio/video recording	Deleted after the required transcript/formal record has been verified unless a documented complaint, investigation, legal claim, quality or safeguarding reason requires longer retention.
Online-search findings	Only relevant findings retained with the recruitment record for the applicable recruitment retention period. Irrelevant search material is not retained.
DBS certificate copy	Not retained longer than necessary. Minimum check and decision information is retained in accordance with safer-recruitment and data-protection requirements.
Suppression record following objection	Minimum information necessary to prevent re-contact, retained for as long as reasonably necessary to honour the objection.
Legal hold / safeguarding / complaint / investigation	The applicable statutory, safeguarding or risk-based period, which may be longer than the normal recruitment period. The reason must be documented.

Appendix 2

Recruitment Data Lifecycle

Stage	Privacy / systems position
Candidate sourced or applies	Recruitment Database record created; source and privacy status recorded.
Initial screening	Limited information collected; Recruitment Team records Suitable to Progress or Not Suitable to Progress.

Stage	Privacy / systems position
Application / Registration	Application form and CV become the formal application record; Registration Pack completed where required. Recruitment Team record Suitable to Progress or Registered but not currently progressing.
Compliance / safer recruitment	Restricted identity, reference, right-to-work, qualification, DBS and other vetting information processed by authorised roles.
Interview panel	Only panel-relevant information released; panel outcome and safeguarding assessment recorded.
Conditional approval / outstanding checks	Outstanding mandatory checks resolved before authority to work.
Staff Database transfer	Required continuing information transferred; staff status may be Active or Inactive. Candidate-only duplicates are reviewed for deletion.
Induction / Tutor Pool	After the required stage, authorised Area Leads may see the relevant matching profile.
Deployment	Final organisation-level and referral-specific gates complete before work starts.
Retention / disposal	Records reviewed and securely deleted, anonymised or retained under legal hold according to Appendix 1 and the Records Management & Retention Schedule.

Appendix 3

Candidate Privacy Principles

- Tell candidates clearly who 1st Staff is and, where their details came from another source, provide the required source information.
- Collect only what is needed for the current recruitment stage.
- Keep capability assessment separate from restricted health, DBS and criminal-record information.
- Use the Recruitment Database for candidate-stage records and the Staff Database for formal staff records; do not use Active/Inactive as the candidate screening outcome.
- Use role-based access so staff see only what they need for their responsibilities.
- Respect objections, callback preferences and requests not to be contacted again.

- Use online searches only for a defined, proportionate safer-recruitment purpose and give candidates an opportunity to explain relevant adverse findings.
- Review AI-generated summaries and transcripts before they become part of the formal candidate record.
- Do not use unapproved AI or transcription tools for candidate information.
- Do not ask prohibited pre-offer health/disability questions; collect reasonable-adjustment information separately where appropriate.
- Keep information accurate, professional, secure and no longer than necessary.
- Use meaningful human judgement for recruitment decisions; automated tools may support administration but do not replace accountable decision-making.
- Escalate any uncertainty about candidate privacy to the Data Protection Officer.

Appendix 4

Minimum Privacy Controls for Interview Panels

- Access candidate information only through approved Company systems and only for the interview purpose.
- Do not forward candidate information to unauthorised recipients or retain copies in personal accounts/devices.
- Keep notes factual, relevant and professionally worded.
- Do not record protected characteristics or sensitive personal information unless genuinely necessary and authorised.
- Where online-search information is provided, consider only the relevant screened finding and give the candidate a fair opportunity to respond where appropriate.
- Record the formal panel decision and rationale in the approved workflow.
- Dispose of temporary notes securely when the formal record is complete.
- Report any accidental disclosure or loss immediately under the Data Breach Procedure.