Home of Professional Excellence

Privacy Policy

Incorporating:

General Data Protection Regulation (GDPR)

Data Protection Act 2018

Cyber Security

Privacy Policy (incorporating GDPR, Data Protection, and Cyber Security)

Procedure Profile	
Procedure Reference Number	
Version	7
Status	Active
Implementation Date	May 2018
Last Review Date	January 2023
The policy will be reviewed and updated as necessary	

INTRODUCTION

This Privacy Policy is the overarching policy for data security and protection for HOPE Superjobs Ltd. (HOPE) and any and all services and registered activities that are conducted under the name of HOPE. These activities and services include:

1. **Children's and Family Contact Centre** – our supervised, supported and hand over service based in Ilford

2. **Domiciliary (Home) Care Service** – our Adults' and Children's services, based in Ilford

3. **Escort and Transport** (in partnership with the London Borough of Redbridge) – based in Ilford

4. **Supported Living/Shared Living Accommodation (Deluxe Care)** – our semi-independent provision based throughout England

PURPOSE

The purpose of this policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulation (GDPR), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

SCOPE

This policy includes in its scope all data which we process either in hard copy or digital copy.

The policy applies to all staff and workers, including temporary workers and any individual or entity with whom we may contract.

PRINCIPLES

HOPE is committed to respecting and to protecting your right to privacy. This Privacy Policy (together with any other of our terms and conditions, and any other documents referred to in them) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read this Privacy Policy carefully to understand our views and practices regarding your personal data and how we will treat it.

We will be open and transparent with service users and clients and those who lawfully act on their behalf in relation to their care and support. We will adhere to the duty of candour outlined in the Health and Social Care Act.

We will establish and maintain policies to ensure we comply with the Data Protection Act (DPA) 2018, the Human Rights Act 1998, the GDPR and the common law duty of confidentiality.

We will establish and maintain policies for the controlled and appropriate sharing of your data and information with other agencies, considering all relevant legislation and individual consent.

We will only use your personal data in the manner set out in this Privacy Policy. We will only use your personal data in a way that is fair to you based on your consent. We will only collect personal data where it is necessary for us to do so and where it is relevant to our dealings with you – as an employee or worker or as a client/service user. We will only keep your personal data for as long as it is relevant to the purpose for which it was collected or for as long as we are required to keep it by law.

We strive to make sure that any and all information we collect from and about you is accurate and correct. We rely on you and others to let us know as soon as possible if there are any changes to the information we hold about you. You should let us know this in writing – by text, email or letter/note. If you choose to update us orally, we will confirm in writing – text, email or letter/note – the changes you tell us about.

We are required to advise you that you have the right to have your data amended to remove errors, to withdraw your consent for some or all processing, and to have you records deleted. For these purposes you should contact HOPE in writing.

You have the right to make a complaint to the regulatory authority, the Information Commissioner's Office (ICO), if you think that your information/data is being incorrectly handled.

The details of the Information Commissioner's Office (ICO) are:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number. Fax: 01625 524 510. Website: https://ico.org.uk

GDPR and BREXIT – UPDATE

On January 1, 2021, the United Kingdom formally and effectively left the European Union (EU).

Although the UK is now "a third country" under the EU's GDPR (i.e., a country outside of the EU without an adequacy decision), on June 28, 2021, the EU adopted an adequacy decision for the UK, ensuring the free flow of personal data between the two blocs for a four-year period (until June 2025).

For UK websites, companies and organisations processing personal data from individuals inside the EU, this UK adequacy decision means unrestricted business-as-usual for the next four years.

After June 2025, the EU will have to engage in a new adequacy process to determine whether the UK still ensures an equivalent level of data protection for the adequacy decision to be renewed.

PERSONAL DATA/INFORMATION HELD BY HOPE

We are HOPE Superjobs Ltd. Our contact details are:

- **Head office**: 3rd Floor, Broadway Chambers, 1 Cranbrook Road, Ilford, IG1 4DU
- T: 020 8553 0827.
- E: Info@hopesuperjobs.co.uk
- **Company registration number**: 508 1894
- **Information Commissioner's Office (ICO) registration number**: Z9489568

Personal data is any information relating to an identified or identifiable natural person (the person is often called a 'data subject'). Data/information could be: a physical or psychological reference; cultural, economic, mental or social identity.

Under the GDPR and Data Protection Act 2018, HOPE is legally bound to document what personal data we hold, where it was obtained, why it is being used/processed, who it is shared with, and for how long it will be held. Most important, HOPE must ensure that this data/information is correct and held securely – and must tell individuals that they have the right to complain – to the Information Commissioner's Office (ICO) – if they think their data is not being handled correctly.

For the purposes of data protection, HOPE Superjobs Ltd. is the data handler and controller for your personal data.

Our Data Protection Officer (DPO) is Ms Irina Irinei. She is supported by an external adviser.

We will hold on to personal information for as long as a staff member or worker or service user or client is with us and in order to meet legal or regulatory requirements, and, amongst others, to resolve complaints or grievances, prevent abuse and fraud.

The tables below capture the above information in a form that makes it easier to understand how and why HOPE collects, may process and retains information, and how it is stored securely. Table 1 is staff information. Table 2 is client/service user information.

Table 1: INFORMATION HELD ABOUT STAFF (OFFICE, CARE/SUPPORT WORKERS)

STAFF - PERSONAL DATA	SOURCE	REASON FOR USE	SHARED WITH	RETENTION PERIOD	REASON FOR RETENTION	PRIVACY/SECURITY (FILED/STORED)
Curriculum Vitae	Individual	Verification / Interview	Internal staff/HR, Regulators/Inspectors	6 years, if recruited / employed. 1 year	Part of personnel information/folder	Personnel folder in secure cabinet, MIS (Birdie, CarePlanner)
Application Form	Individual	Verification / Interview	Internal staff/HR, Regulators/Inspectors	1 year	References, and part of personnel information/folder	Personnel folder in secure cabinet
Copy of Passport/Visa	Individual	Proof of identity, and right to work/remain	Internal staff/HR, Regulators/Inspectors	6 years from end of employment	Part of personnel information/folder. Legal/employment obligation	Personnel folder in secure cabinet
Photograph of individual	Individual	Proof of identity	Internal staff/HR, Regulators/Inspectors	6 years from end of employment	Part of personnel information/folder. Legal/employment obligation	Personnel folder in secure cabinet, MIS (Birdie, CarePlanner)
National Insurance (NI) Number	Individual via P45/P60	Verification	Used by Accounts for salary/wage maternity, and sick pay	3 years after the end of the financial year to which it relates	Income tax regulations, and part of personnel information/folder	Personal folder in secure cabinet
Name & Address (proof of)	Individual via utility bills	Verification	N/A	6 years	Part of personnel information/folder	Personnel folder in secure cabinet, MIS (Birdie, CarePlanner)
Telephone Number(s)	Individual	Communication, contact	Internal staff/HR, Regulators/Inspectors	6 years	Part of personnel information/folder	Personnel folder in secure cabinet, MIS (Birdie, CarePlanner)

STAFF - PERSONAL DATA	SOURCE	REASON FOR USE	SHARED WITH	RETENTION PERIOD	REASON FOR RETENTION	PRIVACY/SECURITY (FILED/STORED)
Disclosure & Barring Service (DBS) Certificate Number	Individual / DBS online	Safeguarding of service users, job role eligibility	Regulators/Inspectors	Certificate valid for one year only.	Inspection, compliance in the health care sector	Personnel folder in secure cabinet, MIS (Birdie, CarePlanner)
Training certificates	Individual	Skills and training needs identification	Internal staff/HR, Regulators/Inspectors	1-3 years, dependent on expiry date,	Proof of skills training	Personnel folder in secure cabinet
Appointment / Termination Letter	HOPE	Verification: Duration of employment	Internal staff/HR, Regulators/Inspectors	3 years	Legal/employment obligation	Personnel folder in secure cabinet
Disciplinary / Grievance	HOPE	Employee relations	Internal staff/HR, external bodies	3 years	Legal/employment obligation	Personnel folder in secure cabinet
Appraisal/Supervision Information	Internal staff/HR	Skills and capability development	Internal staff/HR, Regulators/Inspectors	3 years	Part of personnel information/folder	Personnel folder in secure cabinet
Bank/Building Society Name	Individual	Payment of salary / wage, statutory payments	Internal staff/HR, Accounts	6 years	Part of personnel information/folder. Legal/employment obligation	Personnel folder in secure cabinet + QuickBooks accounts
Next of Kin Name & Address	Individual	Emergency contact	Internal staff/HR	Duration of employment	Part of personnel information/folder	Personnel folder, MIS (Birdie, CarePlanner)
Referee Name & Address	Individual	Employment check	Internal staff/HR	Duration of employment	Part of personnel information/folder	Personnel folder in secure cabinet
Employment Contract	HOPE	Job role, duties, responsibilities	Internal staff/HR		Legal obligation, litigation	Personnel folder in secure cabinet
Health Declaration	Individual	Work environment adjustments/support	Internal staff/HR	Duration of employment	Legal/employment obligation	Personnel folder in secure cabinet
Monitoring Information	Application Form	Equal opportunity; monitoring	HR, Regulators/Inspectors	6 years from end of employment	Part of personnel information/folder	Personnel folder in secure cabinet, MIS (Birdie, CarePlanner)

Table 2: INFORMATION HELD ABOUT SERVICE USERS AND CLIENTS (ADULTS, YOUNG PERSONS and CHILDREN)

SERVICE USER - PERSONAL DATA	SOURCE	REASON FOR USE	SHARED WITH	RETENTION PERIOD	REASON FOR RETENTION	PRIVACY/SECURITY (FILED/STORED)
Name and D.O.B.	L.A. referral document	Verification	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan, risk assessment form, care provision documentation	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Address	L.A referral document	Verification	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan, risk assessment form, care provision documentation	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Photograph	Individual/Rep. or Parent / Guardian	Proof of identity, recognition, Care Plan cover (child)	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan, risk assessment form, care provision documentation	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Telephone Number (Parent / Guardian / Representative)	Individual/Rep. or Parent / Guardian	Communication, contact, call log	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan, risk assessment form, care provision documentation	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Monitoring Information	Individual/Rep. or Parent / Guardian	Equality of provision, personalised management of needs	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision	Part of care plan, and for regulators / inspectors	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in

SERVICE USER - PERSONAL DATA	SOURCE	REASON FOR USE	SHARED WITH	RETENTION PERIOD	REASON FOR RETENTION	PRIVACY/SECURITY (FILED/STORED)
						secure shared drive
Next of Kin Name and Contact Numbers	Individual/Rep. or Parent / Guardian	Emergency contact	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision	Part of care plan, risk assessment form, care provision documentation	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Names of Family Members	Individual/Rep. or Parent / Guardian	Knowledge of who shares residence with or attends individual	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision	Part of care plan, risk assessment form, care provision documentation	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Communication Needs – CARE PLAN	Individual/Rep., Parent / Guardian, Social Services, HOPE planning visit	Provision of personal and individualised care and management of conditions and needs	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan: to provide individual and personalised care	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Personal Hygiene Needs – CARE PLAN	Individual/Rep., Parent / Guardian, Social Services, HOPE planning visit	Provision of personal and individualised care and management of conditions and needs	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan: to provide individual and personalised care	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Medical Needs / Medication – CARE PLAN	Individual/Rep., Parent / Guardian, Social Services, HOPE planning visit	Provision of personal and individualised care and management of conditions and needs	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan: to provide individual and personalised care	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Physical, Dietary,	Individual/Rep.,	Provision of personal	Service staff,	Duration of care	Part of care plan:	Service User folder

SERVICE USER - PERSONAL DATA	SOURCE	REASON FOR USE	SHARED WITH	RETENTION PERIOD	REASON FOR RETENTION	PRIVACY/SECURITY (FILED/STORED)
Recreation and Social Needs – CARE PLAN	Parent / Guardian, Social Services, HOPE planning visit	and individualised care and management of conditions and needs	Involved agencies, Regulators/Inspectors	provision plus 7 years after provision ends	to provide individual and personalised care	in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Details of the Risks Associated with the Individual's Complex Health Care Needs – and How to Manage Them – RISK ASSESSMENT FORM	Individual/Rep., Parent / Guardian, Social Services, HOPE planning visit	Identification of appropriate support, and production of detailed and specific action to take to manage conditions and reduce risk(s).	Service staff, Involved agencies, Regulators/Inspectors	Duration of care provision plus 7 years after provision ends	Part of care plan: to provide individual and personalised care	Service User folder in secure cabinet, MIS (Birdie, CarePlanner) + electronic folder in secure shared drive
Details of educational/training, emotional / behavioural, health and social needs – PATHWAY PLAN	Individual (talk with care co-ordinator), third party (for example, local authority, Barnardo's)	Plan and manage pathway for individual to access benefits, education, employment, training, and gain independence in wider society	Service staff, Involved agencies, Regulators/Inspectors	Duration of support provision plus 7 years after provision ends	Legal requirement	Electronic Service User folder in secure shared drive

LAWFUL REASON FOR PROCESSING/USING PERSONAL INFORMATION/DATA

Tables 1 and 2 provide details of the personal data held by HOPE (its businesses and registered activities), and the reasons for using the information/data.

Staff and Workers

We use and process personal data in order to verify identification, check credentials, check eligibility to work in the UK, check eligibility to work with vulnerable individuals, pay salaries and wages (and other benefits associated with employment, work, and supply of services).

Clients/Service Users

We process personal data in order to: produce care plans or update pathway plans to make sure that individuals receive personal and specific care and support to manage complex conditions and needs; to make sure individuals access the appropriate benefits and wider services; to conduct comprehensive risk assessments and produce risk management plans; to generate correct invoices for care delivery. We are obligated to comply with the requirements of our regulatory body – the Care Quality Commission (CQC), and national association the National Association of Child Contact Centres (NACCC) – in having these processes in place.

Children – and Consent

HOPE does not offer online services to children or any other services other than the delivery and provision of care and support (and all that this involves). We hold information, in order to provide and deliver high quality care and support to children, young people and adults at risk (vulnerable adults) with a range of disabilities, difficulties and complex needs.

Children are defined as those between 0 and seventeen years 11 months (17 years, 11 months). At eighteen (18 years) individuals are classed as young adults.

The GDPR and the Data Protection Act 2018 have set sixteen (16) as the age when a child can give their own consent to the processing of their data. If a child is under 16, parental/guardian consent will be needed. If a child is 16 to 18 but is not capable of giving consent (please see our Mental Capacity and Consent Policy), parental/guardian consent will be needed.

The introduction of the GDPR does not affect or change in any way how we deal and work with children (and their families) in regard to information we hold.

UNDERPINNING POLICIES AND PROCEDURES

This policy is underpinned by the following:

1. Business Continuity Policy
2. Protection of Vital Documents Policy

3. Consent Form for Data Protection/GDPR
4. Record Keeping Policy
5. Document Control, Retention and Destruction Policy
6. DBS (Disclosure and Barring Scheme) Policy and Procedure
7. Code of Conduct of the Company
8. Information Governance Policy
9. Worker Handbook
10. Staff Contracts and Worker Agreement

All the above outline and establish the expected treatment and use of personal data.

SECURITY, CYBER SECURITY AND RISK (AVOIDING BREACHES OF DATA)

Your privacy, and the privacy of your information/data are important to us. We treat all your information as confidential. Personal data is filed and stored securely in the organisation, because of the risk associated with holding sensitive personal data on an identifiable individual. HOPE has ensured the following:

- Hard copy files/folders are stored in lockable cabinets. Access to the data is restricted to staff teams (for example, adults', children', supported living's service staff, contact centre management, senior case workers) and senior managers.

- Access to electronically filed (digital/soft copy) data is password protected (for example, Birdie, CarePlanner, CM2000 MIS).

- Access to the internal shared drive is restricted to office staff only and further restrictions may be imposed by our IT service provider (currently, CHS Networks) at the request of the managing director or senior management team.

- Email is protected through the network by passwords controlled by the IT function. A firewall is in place.

- External sensitive data from commissioning agencies and boroughs is sent through secure email – for example, Egress.

In the event that there is a breach of personal data which could put at risk an individual's freedoms and rights, HOPE is required to notify the person or persons concerned, and also the Information Commissioner's Office (ICO). Risks could be, for example: fraud/financial loss, due to accessing a service user's financial information; or loss of confidentiality.

INDIVIDUALS' (YOUR) RIGHTS AND ACCESS TO YOUR INFORMATION

The General Data Protect Regulation and Data Protection Act 2018 gives individuals (you) rights regarding information/data held about you. In relation to your relationship with HOPE – either as an employee, a worker, a service user or client, you have the following rights which we will uphold:

Your right	Comment
• To be informed	You may be told (informed about) what information we hold on you. Please refer to tables 1 and 2.
• To have access to your information	You may request copies of information we hold, and we will have 28 days to comply (provide the information), unless your request has no basis or is excessive. You may be charged for a request for information, if your request is excessive. Your request may be refused, and we will tell you why within one month of your request. If your request is refused, you have the right to complain to the Information Commissioner's Office (ICO) whose address and contact details are on page 5 of this policy document.
• To data/information portability	You may obtain your personal data from us and re-use it for your own purposes.
• To rectification (putting something right)	Incorrect information we hold about you will be corrected or put right (rectified).
• To erasure (deletion, removal)	Information we hold about you may be deleted or removed subject to regulatory or statutory requirements that HOPE must comply with.
• To object	You may not like the fact that we hold information about you, and you may want to tell us this. We will make a file note of your objection.

We store information necessary to ensure safe delivery of care to our service users. We process information to ensure correct payment (such as salary or wage) is made to identifiable persons/staff and workers.

DATA PROTECTION BY DESIGN AND BY DEFAULT

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

Any new high-risk data processing activities will be assessed using a (Data) Privacy Impact Assessment (DPIA) before the processing commences. Please see, also, our Privacy Impact Assessment Procedure.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work for which it is required, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

RESPONSIBILITIES

Our Data Protection/GDPR Officer (DPO) is the manager of the Children's and Family Contact Centre – Irina Irinei.

Our Register Manager and managing director of HOPE is our overall Data Protection Champion.

Both the DPO and the managing director have access to expert external specialists in general data protection specific to the health and social care sector.

CONTACTING US:

HOPE Superjobs Ltd.

- **Head office**: 3rd Floor, Broadway Chambers, 1 Cranbrook Road, Ilford, IG1 4DU
- T: 020 8553 0827.
- E: Info@hopesuperjobs.co.uk
- **Company registration number**: 508 1894
- **Information Commissioner's Office (ICO) registration number**: Z9489568

SUMMARY

Your privacy and the privacy of any information we hold about you are important to us. We do everything in our power to keep your data safe and secure. We use your information only to in the ways outlined in tables 1 and 2 in previous pages. You have rights where your information/data is concerned, and those rights are outlined in this policy. HOPE will never share your information with a third party, apart from the reasons outlined in tables 1 and 2, and elsewhere in our Data Protection Consent Form, and any privacy notices.

This policy is the overarching policy for the range of regulated activities undertaken under the umbrella of HOPE Superjobs Ltd. Regulated activities may have specific policies and procedures to underpin their operation(s).

This policy has been approved by the Registered Manager who is also the Managing Director of HOPE.

Signed: 

Marlene Joseph, Managing Director

How UK and EU legislation dovetail to ensure the protection of individual data, and privacy:

Brexit, GDPR and the DPPEC regulations

The GDPR/Brexit changes made to UK data privacy law are all contained in the government's *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*, also known as the DPPEC regulations.
They took effect on January 31, 2020, in accordance with the now-passed EU Withdrawal Agreement.

The **DPPEC regulation**s do two major things:
1. create a whole "new" domestic law known as UK-GDPR.
2. revise the Data Protection Act 2018.

In order to keep the promise in the Withdrawal Agreement's Articles 70-73, the UK has decided to create a whole "new" domestic law known as the **UK-GDPR** (United Kingdom General Data Protection Regulation).

The new UK-GDPR is essentially the same as the European GDPR.

It is literally made from the same law text as the EU GDPR but amended so as to substitute the parts of text that read *EU* and *Union law* with *UK* and *domestic law*.

The UK-GDPR merge the two pre-existing regimes for personal data protection – namely that established by the European GDPR and that established by the Data Protection Act 2018 (specifically the parts of that law known as the "applied GDPR"). The DPA2018's "applied GDPR" section is the one that extended the GDPR's standards to areas that were out of scope of EU law and the GDPR, namely that of **law enforcement**, **intelligence services** and **immigration** (among others).

The amended Data Protection Act 2018

The new and amended Data Protection Act 2018 also took effect on January 31, 2020. The DPA2018 will no longer rely on the EU GDPR, but on the UK-GDPR instead. It will instead refer to the new domestic GDPR after Brexit.

UK citizens will now be protected by a comprehensive data protection regime that is made up of the UK-GDPR on the one hand that defines (just as the EU GDPR does today) what personal data is and how it is allowed to be processed, and the Data Protection Act 2018 on the other hand, supplementing the domestic GDPR and extending beyond it as well.