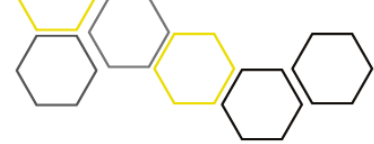


Start360

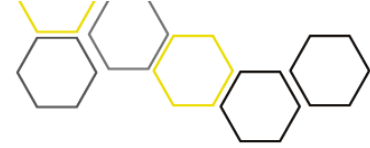


GDPR, Data Protection and Privacy Policy



Contents

| | |
|---|----|
| Contents | 2 |
| Control Record | 3 |
| Review History | 3 |
| 1. Introduction..... | 4 |
| 2. Purpose of Policy | 4 |
| 3. Values and Principles | 5 |
| 4. Compliance | 5 |
| 5. What Compliance means | 7 |
| 6. Incident Response | 8 |
| 7. Monitoring and Review | 8 |
| 8. Appendix 1 - Employee Data | 10 |
| 9. Appendix 2 - Client data | 12 |
| 10. Appendix 3 - Subject Access Request ("SAR") | 13 |
| 11. Appendix 4 – Service User Privacy Notice | 14 |



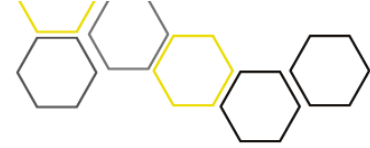
Control Record

Review History

| Version | Date Reviewed | Brief Summary of Change | Owner's name |
|---------|---------------|---|--------------|
| 1 | January 2021 | New policy developed. | SLT |
| 2 | March 2024 | Amendments: Amended title to reflect the document's use as a Privacy Policy. Compared policy to ICO requirements for a Privacy Policy to confirm meets these requirements. Included Service User Privacy Notice as Appendix 6. | SLT |
| 3 | November 2024 | Key changes focused on clarifying where operational and Board responsibility lies, using specific definitions as legislation requires, redefining the terminology for a Data Protection Officer to Data Protection Champion, redefining the importance and process for compliance, removal of certain wording/sections where not required (e.g. technical & operational compliance narrative and references to sources of information), greater specification added around Subject Access Requests including required fees and identity evidence, and clarification on retention periods. | SLT |

Overview

| | |
|--|-----------------------------|
| Policy ID | 25.3 |
| Author | SLT |
| Publication date: | 04/11/24 |
| Approved by: | Board |
| Effective from: | 04/11/24 |
| For attention of and action by: | Board, Staff and Volunteers |
| Review date: | 04/11/27 |



1. Introduction

Start360 is committed to protecting the rights and privacy of individuals and the purpose of this policy is to communicate our position on the protection of personal data. It is a set of principles, rules and guidelines that informs how we will ensure ongoing compliance with data protection laws specified as the:

- Data Protection Act 2018, which is the UK's implementation of the General Data Protection Regulation (GDPR) (referred to as DPA) and;
- General Data Protection Regulation (Regulation (EU) 2016/679) referred to as GDPR.

| | |
|-----------------------------|--|
| Overview | To demonstrate compliance with the DPA 2018 and GDPR legislation and to summarise Start360's roles and responsibilities relating to Data Protection. |
| Scope | This policy applies to all personnel whether staff, contractor, third parties or members of partnership organisations with access to Start360's data or information systems and/or assets. |
| Implementation & monitoring | Data Protection Champion Data Controller Senior Management Team |
| Risk implications | Financial, reputational due to failure to comply with the DPA 2018 and GDPR legislation. |

Definition of personal data

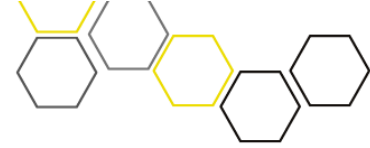
Personal data is defined by the DPA as information that relates to an identified or identifiable individual.

The Act also defines "**special category personal data**" and further information is included in Appendices 1 and 2.

2. Purpose of Policy

Personal information, whether held on paper, on computer or other media, is subject to the legal safeguards specified in the DPA and the GDPR. Start360 is committed not only to the letter of the law but to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

The purpose of this policy is:



- to clearly define Start360's commitment to protecting personal data; Start360 acts as a data Controller/Joint Controller and a data Processor. We are registered as a data controller with the Information Commissioner's Office.
- **Data Controller:** a person that decides how and why to collect and use the data. The controller must ensure that the processing of data complies with data protection law.
- **Data Processor:** a separate person or organisation (e.g. sub-contractor, pension provider etc.) who processes data on behalf of the controller and in accordance with their instructions. Processors have direct legal obligations but are more limited than the controller's obligations.
- Start360 has a Data Protection Champion - Director of Corporate Services.

3. Values and Principles

Start360 need to process certain personal data about employees, clients and other stakeholders (including service users) in order to fulfil its purpose and to meet its legal obligations to funding bodies and the government. Examples of data include:

- HR: recruitment and payment of salaries, expenses, pensions and other benefits.
- Service users: equal opportunities monitoring, attendance, assessment records and payment of expenses such as EMA or travel assistance.
- Suppliers: day to day purchasing and sale of goods (business to business, sole traders etc).
- Customers: making or receiving of payments as part of day-to-day trading.
- Funders: monitoring and evaluation of service users for reporting purposes (see privacy notice)
- Complying with legal obligations and government including health and safety legislation such as The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (Northern Ireland) 1997.
- Personal details of Board members.

For further information see Appendices 1 and 2 which outline the personal data held by Start360 relating to employees and service users.


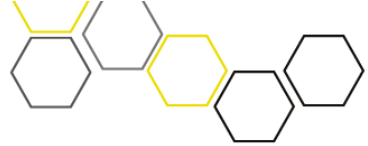
To comply with legal obligations, Start360 ensures all information about individuals is collected and used fairly (only for the stated collection purpose), stored safely and securely, retained for the minimum necessary time period and not disclosed to any third party unlawfully.

4. Compliance

To comply with its obligations, we undertake to adhere to the following eight principles:

1) Process personal data fairly and lawfully (the right to be informed)

- Start360 will make all reasonable efforts to ensure that individuals who are the focus of personal identifying information are provided with the following:
 - the name of the data controller.

- 
- 
- the purposes of the processing of their data.
 - any disclosures to third parties that are envisaged.
 - an indication of the period for which the data will be kept, and;
 - any other information which may be relevant.
- Start360 will ensure the data is adequate, relevant, and not excessive in relation to the purpose for which it is processed. We will not collect personal data which is not strictly necessary for the purpose for which it was obtained.
 - Start360 will process the data for the specific and lawful purpose for which it was collected. We will ensure that the reason the data was originally collected is the only reason for which we process that data unless the individual consents to any additional processing before it takes place.
 - Start360 undertake not to disclose personal data to unauthorised third parties. Legitimate disclosures may occur in the following instances:
 - where the individual has given their consent to the disclosure.
 - To statutory bodies e.g. HMRC
 - the disclosure is required for the performance of a contract.

2) Subject Access Rights (SARs) (the right of access)

Individuals have a right to access personal data relating to them which is held by Start360. The organisation will use reasonable efforts consistent with our legal duty to supply, correct or delete personal information about an individual on our files.

- If an individual wishes to exercise this right, please submit a request to the Data Protection Champion.
- A staff member receiving a SAR should forward it to the Data Protection Champion.

For further information please refer to Appendix 3.

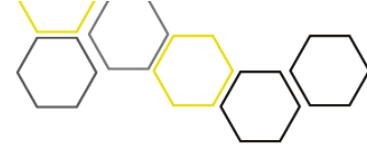
3) Keep personal data accurate (the right to rectification)

It is the responsibility of the individual giving their personal data to ensure it is accurate. If there is a change in circumstances meaning that the data needs to be updated, the individual should notify Start360 immediately. It is the responsibility of Start360 to ensure that any notification regarding the change is noted and acted on.

4) Only keep personal data for as long as is necessary (the right to erasure)

Start360 undertake not to retain personal data for longer than is necessary to ensure compliance with GDPR legislation and other statutory requirements.

To comply we will undertake a regular review of the information held and monitor the deletion and retention as required. Start360 will dispose of any personal data in a way that protects the rights and privacy of the individual concerned.



5) Restrict the processing of personal information

At any time, an individual can request to know what information is stored and request action to rectify, block, erase or delete inaccurate information while that process is underway.

Individuals have the right to prevent processing of information if the information is subject to corrective action.

6) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Start360 will not transfer data to such territories without the explicit consent of the individual. This includes publishing information on the Internet because transfer of data can include placing data on a website that can be accessed from outside the EEA therefore Start360 will always seek the consent of individuals before placing any personal data (including photographs) on its website.

If Start360 collects personal data in any format via its website, it will publish a clear and detailed privacy statement prominently on the website, and on other sites wherever personal data is collected.

7) The right to object allows an individual to request that processing is prevented. Start 360 commit to the formal consideration of and feedback on each request within appropriate timescales.

8) Rights in relation to automated decision making and profiling

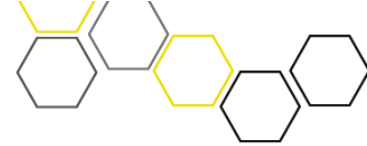
- Currently Start360 do not conduct any automated individual decision making or profiling. Any move towards the consideration of this will be subject to a robust data protection impact assessment.

For details of Technical & Operational Compliance for employees, agents, contractors, or other parties working on behalf of Start360 please refer to Appendix 4.

5. What Compliance means

Start360 will:

- ensure that the legal basis for processing personal data is identified in advance and that all processing complies with the law.
- not do anything with your data that you would not expect given the content of this policy and the fair processing or privacy notice.
- ensure that appropriate privacy notices are in place advising employees and others how and why their data is being processed and advising individuals of their rights.
- only collect and process the personal data it needs for purposes identified in advance.
- ensure that the personal data it holds is accurate, or a system is in place for ensuring that it is kept up to date as far as possible.



- only hold onto personal data for as long as it is needed, after which time Start360 will securely erase or delete the personal data – Start360's Data Protection Champion will set out the appropriate period of time. Funders may also designate specific retention periods Start360 is required to adhere to.
- ensure that appropriate security measures are in place so that personal data can only be accessed by those who need to access it and that it is held and transferred securely.

The organisation will ensure that all staff who handle personal data on its behalf are aware of their responsibilities under this policy and other relevant data protection and information security policies, and that they are adequately trained and supervised.

Third parties

Third parties (e.g. sub-contractors, agencies etc) working with Start360 who have access to personal information will be expected to read and comply with this policy. Departments who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which include an agreement to abide by this policy.

6. Incident Response

As a data controller, Start360 is required to notify the Information Commissioner's Office that it is processing personal data.

Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place. The Data Protection Champion shall be responsible for notifying and updating the Information Commissioner's Office, however responsibility for updating the Champion rests with all impacted Staff.

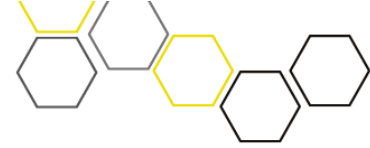
Breach of personal data

Under GDPR we have a duty to formally risk assess and to report certain types of personal data breach to the relevant supervisory authority (the ICO). Start360 will do this within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, Start360 will also inform those individuals without undue delay.


7. Monitoring and Review

- This policy will be updated as necessary to reflect best practice in information management, security, and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.
- This policy will be regularly monitored and Start360 will review in line with the policy review timeframe.



- This policy will be reviewed in response to adoption of emerging technologies and /or implementing new work streams

For help or advice on any data protection or freedom of information issues, please do not hesitate to contact The Data Protection Champion and or the ICO.



8. Appendix 1 - Employee Data

Start360 holds the following personal data relating to employees:

- Identification information including, but not limited to, names and contact details.
- Equal opportunities monitoring information including age, gender, race, nationality, and religion. Such information shall be anonymised wherever possible.
- Health records including details of sick leave, medical conditions, disabilities, and prescribed medication.
- In case of emergency contacts provided
- Employment records including, but not limited to, interview notes, curricula vitae, application forms, assessments, training, performance reviews and similar documents.
- Details of salaries including increases, additional hours, benefits, and expenses.
- Records of disciplinary matters including reports and warnings, both formal and informal.
- Details of grievances including documentary evidence, notes from interviews, procedures followed and outcomes.
- Potential conflict of interest information including any information on any previous employment in which employees continue to have a financial interest or alternative employment outside of Start360 e.g. sessional work or any self-employed or paid work.
- Potential conflict of interest information from appointments (voluntary or otherwise), membership of any professional bodies, special interest groups or mutual support organisations, investments in unlisted companies, partnerships and any other forms of business, major shareholdings.
- Any other potential conflict of interest information not covered in the categories above.

Employee benefits

It may be necessary for third party organisations to collect personal data relating to relevant employees in cases where employees are enrolled in benefit schemes such as:

- NEST Pension Scheme
- BHSF Healthcare Scheme
- Trade Union (for fees deducted at payroll)

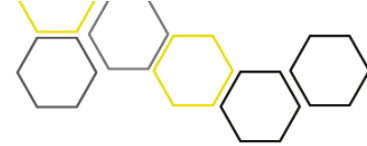
Prior to collection, employees will be fully informed of the personal data that is to be collected, the reasons for its collection, and the way(s) in which it will be processed.

Start360 shall not use any such data except insofar as is necessary in the administration of relevant benefits schemes.

Employee monitoring

Start360 may from time to time monitor the activities of employees. Such monitoring may include, but will not necessarily be limited to CCTV, internet, and email monitoring. In the event that monitoring is to take place employees will be informed in advance (unless exceptional circumstances justify covert monitoring e.g. circumstances involving the investigation of criminal activity or a matter of equal severity).

Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.



Monitoring will only take place if Start360 considers it is necessary. And data collected during such monitoring will only be collected, held, and processed as necessary.

Start360 shall make all reasonable endeavours to ensure there is no intrusion upon employees' personal communications or activities. Monitoring will not take place outside of the employee's normal place of work or work hours unless the employee is using Start360's equipment, availing of blended working locations or other facilities including, but not limited to, organisation email, intranet or a virtual private network ("VPN") service provided by Start360 for the employee's use.

Special category personal data

The DPA includes the following personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of identifying an individual
- an individual's health
- an individual's sex life or sexual orientation

Personal data about criminal allegations, proceedings or convictions is not special category data. However, there are similar rules and safeguards for processing this type of data, to deal with the particular risks associated with it.

Start360 processes special category data of employees as is necessary to comply with employment and social security law (e.g. PAYE, pensions, student loans, healthcare, sickness pay, maternity, paternity, adoption leave etc).

In addition, employers in N.I. must comply with The Fair Employment and Treatment (NI) Order 1998 and the Fair Employment (Monitoring) Regulations (NI) 1999 which introduced a number of additional monitoring requirements for all registered employers. Employers who employ 11 or more people working more than 16 hours a week must register with the Equality Commission for Northern Ireland.

This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above.

Start360's Data Controller adheres to the guidance relating to data retention for employees, past employees and staff recruitment and sets out how long special category data will be retained.



9. Appendix 2 - Client data

Start360 only holds personal data that is directly relevant to its dealings with a given data subject. That data will be collected, held, and processed in accordance with the data protection principles and with this Policy.

Client data

The following data may be collected, held, and processed by Start360 for clients:

- Identification information including, but not limited to, names and contact details.
- Equal opportunities monitoring information including age, gender, race, nationality, religion; sexual orientation, disabilities, and relationship status, etc.
- Attendance records.
- Client expenses such as EMA or financial travel assistance.
- Client session notes and action plans.
- Results of assessment and other diagnostic tools.
- Record of client issues.
- Record of involvement with the Justice System.
- Surveys relating to client experiences with the service/organisation.
- Record of any correspondence to and from the client.
- Family data where relevant.

Research

Anonymised client scores may be held for an extended period to facilitate longitudinal research.

Special category personal data

The DPA includes the following personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- the processing of genetic data, biometric data for the purpose of identifying an individual
- an individual's health
- an individual's sex life or sexual orientation

Personal data about criminal allegations, proceedings or convictions is not special category data. However, there are similar rules and safeguards for processing this type of data, to deal with the particular risks associated with it.

Start360 processes special category data of clients, and third parties as is necessary to meet funders' requirements and to comply with equality legislation relating to disabled service users and for the establishment, exercise or defence of legal claims.

Start360's Data Controller adheres to the guidance relating to data retention and sets out how long special category data will be held onto.



10. Appendix 3 - Subject Access Request (“SAR”)

A data subject may make a subject access request at any time to find out more about the information which Start360 holds about them.

- SARs can be made in writing and addressed to:

Corporate Services Manager

Start360

6-10 William Street

Belfast

BT1 1PR

- A SAR should be clearly identifiable as a SAR.
- SARs must make it clear whether it is the data subject themselves that is making the request or whether it is a person acting on his or her behalf.
- In a case where individual identity isn't clear; proof of identity must be provided. If the SAR is made on another's behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject.
- Start360 currently requires a fee appropriate to the administrative costs of complying with a request where excessive information is requested. The fee can be paid by BACs or a cheque.

Upon receipt of a SAR Start360 shall have a maximum period of 1 month within which to respond fully. The following information will be provided to the data subject:

- Whether or not the organisation holds any personal data on the data subject.
- A description of any personal data held on the data subject.
- Details of what that personal data is used for.
- Details of how to access that personal data and how to keep it up to date.
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.



11. Appendix 4 – Service User Privacy Notice

1. Introduction

This Service User Privacy Notice tells you what we do with your personal information when you access services from Start360.

Data protection is a fundamental right. The European Union General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA 2018) govern our use of personal data and ensure that your rights are protected.

Start360 understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of all our service users and will only collect and use personal data in a way that is consistent with our obligations and their rights under the law.

2. What do we collect and what do we use it for?

Personal data is any information from which you can be identified directly or indirectly. Start360 processes the following about you:

Your **contact details** – such as your name, address, phone numbers, next of kin etc so that we can contact you.

Your **referrer's contact details** – so that we can inform them of your progress.

Your **equality profile** – such as your gender, age, disability to monitor the equity of our delivery client profile on who benefits from our services.

Your **relevant medical details** – such as medication that may need to be taken, allergies or other health conditions to ensure we can take the best care of you in the case of an emergency and so that we can tailor our services to meet your needs.

Your **engagement details** – including referral details summarising your need for services, relevant issues you may have faced in your life, ongoing session notes and dates, and attendance record, so that we have an accurate record of your engagement with us.

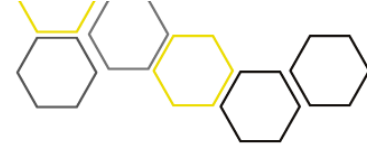
Your **assessment details** – such as your assessment baseline scores or feedback surveys so that we can monitor your progress and the performance of the service.

Your **bank details** – for services which require us to process statutory payments or expenses.

Other details as required by services such as National Insurance numbers, Unique Learner Numbers and Prison ID's.

Some of your information will be retained for research and development reporting purposes. This will usually be anonymised, but your consent will be obtained if you will be named in any of these reports that may be kept longer term.

We also collect, use and share aggregated data such as statistical or demographic data which we collect from interactions with our service users. This is used for management monitoring reports and general research purposes. Aggregated data may be derived from personal data but since it cannot be used to identify an individual, it is not personal data.



3. Purpose and legal basis for processing

Start360 is a company registered in Northern Ireland, with registered office at 6-10 William Street, Belfast, BT1 1PR. Our company number is NI033207, and charitable number is NIC105848.

In order to provide our services, we need to process personal and special category data. Start360 is the **controller** for information about you that is collected and held when you are accessing Start360 services.

Under GDPR, we must always have a lawful basis for using personal and sensitive data. This may be because the data is **necessary for our delivery** of services to you, because you have **consented** to our use of your personal data, or because it is in our **legitimate business interests** to use it.

As part of our services we may be required to transfer some personal data to other people such as advising the person who referred you about your progress and if you have attended your appointments.

For some services, Start360 is a **processor** for certain information which means that we are processing that data on behalf of (and in accordance with the instructions of) another organisation. For example, Start360 is a processor in respect of processing Educational Maintenance Allowance payments for some employability related services.

4. How do we secure your personal data?

It is our policy to ensure that all personal data held by us is handled correctly and appropriately according to the nature of the information, the risk associated with mishandling the data, including the damage that could be caused to you as a result of loss, corruption and/or accidental disclosure of any such data, and in accordance with any applicable legal requirements.

We take appropriate physical, electronic and managerial measures to ensure to keep your information secure, accurate and up to date. Sensitive information is always locked away and only suitably trained, authorised personnel can access it.

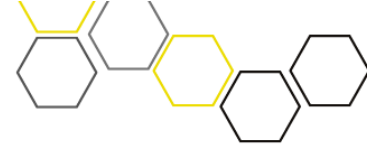
5. How long will we keep your data?

We only keep it as long as reasonable and necessary. Some parts of your information such as your postal area, reported issues, assessment scores and survey scores may be kept longer to inform our longitudinal research into the effectiveness of our interventions. This will be anonymised. We may have to retain some other information for legal reasons.

Some funders stipulate a data retention period in their contract, and we have a duty to comply with this. Where a funder does not stipulate any retention period, we will dispose of your data 7 years after the funding for the service has ended (with the exception of the information in the above paragraph which is held for longitudinal research purposes). Data on any financial transactions will be kept for seven years in accordance with financial legislation.

When we no longer need information, we will always dispose of it securely, using specialist companies, if necessary, to do this work for us.

We may store aggregate data without limitation on the basis that no individual can be identified from the data.



6. Will we share your information with anyone else?

We may transfer the information to other staff members, if for instance you are referred internally to another service or to another practitioner in the same service.

Your case details may be shared with your practitioner's line manager in performance management reviews to ensure the staff members are offering you the best possible care. Your name will be anonymised in any written staff performance management records held by the organisation.

We may also share your information with your referral agent to keep them informed of your progress and to other third-party organisations involved in your care.

Where information needs to be shared outside our organisation, Data Sharing Agreements will be put in place as necessary by the Controller to ensure compliance with the data protection regulations.

7. What rights do you have about the personal data we collect and hold?

You have certain rights under data protection law:

Right to be informed. You have the right to know how we use your personal information in clear and transparent language.

Right of access. You have the right to know and have access to the personal data we hold about you (more about this below).

Right to data portability. You have the right to receive your personal data in a common and machine-readable electronic format.

Right to be forgotten. You have the right to request to have your personal data erased.

Right to rectification. You have the right to have your personal data corrected where it is inaccurate or incomplete.

Right to object. You have the right to object to our processing.

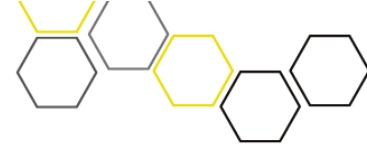
Right to purpose limitation. You have the right to limit how we use your personal data in certain circumstances.

Rights related to automated decision-making and profiling. You have the right to ask for any automated decisions to be reviewed by an individual.

Though these rights depend on our reason for processing your information, they must be protected. We are committed to upholding your rights in line with the law. The Information Commissioner's Office provides advice and information on how to exercise these rights.

You can contact the Data Protection Champion for further clarification or about any concerns you might have. You can contact the Data Protection Champion in writing to 6-10 William Street, Belfast, BT1 1PR or by email to info@start360.org.

You also have the right to lodge a complaint with the Information Commissioner's Office, which upholds data protection rights: <https://ico.org.uk/concerns>



8. What happens if you no longer want us to process personal data about you?

If we are holding personal data about you as a processor, we will need to transfer your request to the controller who has engaged us to provide our services.

If we are holding personal data about you as a controller, we will comply with your request unless we have reasons for lawfully retaining data about you.

If we are holding personal data about you and using that data for marketing purposes or for any other activities based on your consent, you may notify us at any time that you no longer want us to process personal data about you for particular purposes or for any purposes whatsoever and we will stop processing your personal data for that purpose. This will not affect your ability to receive our services.

9. Accessing your personal data

You have the right to get a copy of some information held about you.

If you want a copy your personal data held by us, you should make your request in writing to the Data Protection Champion who will ensure that your request is carried out in line with your rights. Any request should be made to the Data Protection Champion in writing at 6-10 William Street, Belfast or by email to info@start360.org. You may be required to prove your identity.

You will receive a response promptly and within one month. There may be a cost of £10 for the administrative costs of complying with a request.

10. Changes to this privacy notice

We may change this privacy notice from time to time by updating this page to reflect changes in the law, the type of work we do, and our privacy practices. The most up to date copy of our privacy notice will always be available on our website.

If you have any questions about this notice, feel free to send us an email to info@start360.org.