

Introduction

SHIELD ("the service") is integrated into *NTU Psychology*, which is one of the *departments within the School of Social Science* at Nottingham Trent University ("NTU").

SHIELD is committed to protecting the privacy and security of your personal information. This Privacy Notice provides important information about the service and NTU. *SHIELD* is physically located within the NTU city campus.

For the purpose of this Privacy Notice references of "we" or "us" relates to the *SHIELD* service as a part of NTU. This Privacy Notice identifies and manages how we deal with our Data Protection responsibilities in accordance with our legal and regulatory obligations.

SHIELD encourages you to review the privacy statements of any websites you choose to navigate to from the *service's* website (or navigate from to our website) or digital services that we provide links to so that you can understand how those websites collect, use and share your information as well. Any third-party sites that you can access through the website are not covered by this Privacy Notice and we accept no responsibility or liability for these sites.

Who we are

NTU is the data controller for *SHIELD* data. We are responsible for deciding how we hold and use personal information about you.

This Privacy Notice applies to any *SHIELD* enquirers, clients or users ("you" or "your") or services that link to it (collectively, our "Services"). It should be read in conjunction with any other NTU privacy notices that apply to you depending on your circumstances, such as:

- [Nottingham Trent University](#)
- [Website and Cookies](#)

Please read this Privacy Notice carefully and contact our Data Protection Officer if you have any questions about our privacy practices or your personal information choices.

Data Protection Officer

Nottingham Trent University Address: 50 Shakespeare Street, Nottingham, NG1 4FQ

Email: DPO@ntu.ac.uk

Alternatively, please email the *SHIELD* Director or Manager at shield@ntu.ac.uk who may be able to assist.

We may need to update this Privacy Notice from time to time. Where appropriate, we will notify *SHIELD* users of such changes.

Personal Information

SHIELD is committed to the responsible handling and protection of personal information.

Personal Data, or personal information, means any information about an individual from which that person (a “Data Subject”) can be identified. It does not include data where the identity has been removed (anonymous data). The information will be Personal Data if a person can be identified either directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For example, personal data may include names, addresses, email addresses and telephone numbers; it may also include images in photographs or films and recorded telephone conversations.

Why we process your data

We collect, use, disclose, transfer, and store personal information to provide services to you and for our operational and business purposes as described in this Statement. We want to be clear about our privacy practices so that you are fully informed and can make choices about the use of your information, and we encourage you to contact us at any time with questions or concerns. You can email the Data Protection Officer at DPO@ntu.ac.uk or SHIELD Director or Manager at shield@ntu.ac.uk.

The types of personal information we collect

The categories of personal information that we may collect, store and use about you include (but are not limited to):

- Name, phone number, email address,
- Date of birth and gender;
- Any disability/access requirements
- *If you are submitting a referral*, your job title;
- Information relating to the matter in which you are seeking support from us, such as academic attainment;
- Communications with you for the purpose of accessing the Service, management of any issues arising in the course of the Service provision, and any follow up communications following participation in the Service;
- Audio and video conferencing recordings, including of coaching sessions;
- Information inputted by you and/or your coach into the SHIELD app, such as the adolescent avatar, worry tree, support street and any notes;
- Evaluation data for SHIELD provided by you for service evaluation and development purposes;
- Visual images (including live stream CCTV).

In some circumstances, we may need to process sensitive personal information or special category data which may include (but is not limited to) your ethnic origin, political opinions, religious or similar beliefs, your physical or mental health, your sexual orientation and personal data relating to criminal offences and convictions. We will only collect this information where you elect voluntarily to disclose it to us.

Where you choose to disclose special category data to us, we may process it for the following purposes:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or comply with relevant legislation.

- Where it is needed in the public interest, such as for equal opportunities monitoring.
- Where it is needed to investigate student behaviour (under our Student Code of Behaviour).
- Where it is data that you have already made public.
- Where it is necessary to do so to establish, exercise or defend legal claims.
- Where the processing is necessary for archiving purposes in the public interest, or for scientific or historical research purposes, or statistical purposes.

To discuss the purpose for which any particular use of data has taken place, please contact us using the details provided above.

How we collect your data

We typically collect personal information about students of NTU, clients, users and *referrers* to our Services directly, to maintain data accuracy, to provide and enhance the Services, and to manage and fulfil NTU processes and obligations.

Apart from the data that you provide to us, we may also process data about you from a range of sources, which include:

- Data that we and our staff generate about you, such as client notes made by our students on the SHIELD app, scheduling records, and information in connection with your attendance at SHIELD;
- Email and telephone correspondence you have with us;
- Records of any potential conflict of interests;
- Data supplied by third parties such as referral agents, or NTU and our partners;
- Data supplied through our Digital Services: which are the SHIELD app domain <https://shield.ntu.ac.uk> and any other NTU-authorized internet services, websites, products, social media, mobile phone apps and/or software applications that enable you to use, access, view, listen to and/or download NTU content or to interact with us online (or through any other digital means) on any device. We collect information that you provide to us by filling out forms on the website or by corresponding with us through the Digital Services. It includes information that you provide when you participate in discussion boards or other social media functions within the Digital Services, enter a competition, promotion or survey, and when you report a problem with the Digital Services.

We will collect additional personal information in the course of the provision of Services to you, throughout the period you receive support sessions on SHIELD.

Our servers, logs, and other technologies automatically collect certain information to help us administer, protect, and improve our Services; analyse usage; and improve users' experience.

As part of NTU, *SHIELD* uses NTU's IT and other systems, and has appropriate arrangements in place to enable this. This means that, whilst you may deal directly with *SHIELD staff*, your personal data will technically be stored on secure and specific servers within NTU

We receive and store certain types of information whenever you interact with us. This includes the use of "cookies". Please refer to our cookies policy available at [Nottingham Trent University | Cookies](#) for further information regarding our use of cookies. We may also automatically record visits to our website for the purposes of improving our services. These

recordings may record mouse clicks, mouse movements, page scrolling and any text keyed into website forms. Information collected by cookies or session recordings is stored and is used for aggregated and statistical reporting.

NTU uses CCTV around campus and will collect and store information. For full details of our CCTV use, please refer to our [CCTV Policy](#). We do use CCTV within the SHIELD clinic but only on a live feed to help clinical supervisors identify coaches who require assistance, none of the CCTV within the SHIELD clinic is saved or stored.

How we use data about you

When processing personal data, we rely on a combination of the grounds permitted by data protection law, depending on whether you are a client or member of NTU (including students undertaking activities *on SHIELD*):

- The processing is necessary for us to perform a contract we have with you, or because you have asked us to take specific steps before entering a contract. Examples of processing include in the case of *SHIELD* clients:
 - the operation and delivery of *support you have been referred to us for*, including scheduling appointments and enquiries; and
 - *in the case of NTU students*, for the administration of your studies.
- The processing is necessary of a public task or a task in the public interest (for example, the provision of teaching and research by a University is a public task in the public interest). Examples of this kind of processing include:
 - Supervision and teaching of NTU students participating in SHIELD.
- The processing is necessary for our legitimate interests (for example, we have a legitimate interest in being able to perform our services optimally and efficiently), or the legitimate interests of a third party, and there is no reason to protect your personal data which overrides those legitimate interests. Examples of this kind of processing include:
 - to notify you about changes to our services;
 - to provide management statistics through research using student and client data which may be used by us to enhance the SHIELD experience and enhance our service provision;
 - to provide you with information on research projects which may be of interest to you.
- The processing is necessary for us to comply with any statutory or legal obligation to which we are subject. Examples of processing include:
 - to ensure we comply with our obligations *under GDPR* and other regulatory or statutory bodies (as applicable); and
 - to ensure compliance with legislation (eg the Prevent Duty under the Counter Terrorism & Security Act 2015).
- In rare circumstances, where you have given consent for us to process your personal data.
- In limited cases, we may also process data where it is necessary to protect someone's "vital interests" (either the data subject, or another person). Disclosures may be made to external parties to ensure the safety and wellbeing of individuals; for example, we may share your contact details with emergency health services if you are taken unwell while on the premises.

Where special categories of personal data are processed, additional legal bases for processing are required – see "**The types of personal information we collect**" for those applicable to SHIELD. :

- We do not carry out automated processing using the data that you have supplied to using relation to SHIELD.

Who we share your data with

We do not, and will not, sell personal data to third parties. We will only share it with third parties external to SHIELD if we are allowed or required to do so by law.

We may share or disclose personal information when necessary to provide the Service or otherwise conduct our operations. When we share personal information, we do so in accordance with data privacy and security requirements. We may occasionally share non-personal, anonymised or pseudonymised, and statistical data with third parties.

Examples of bodies to whom we may be required by law to disclose certain data

- include, but are not limited to: Agencies with responsibilities for the prevention and detection of crime, apprehension and prosecution of offenders: We may be required to use and retain personal information for legal and compliance reasons, such as the prevention, detection, or investigation of a crime; loss prevention; or fraud;
- Governmental, audit or regulatory bodies: We may use personal information to meet our external audit, regulatory or governmental obligations;
- Legal system entities: We may use personal information where required to enforce our terms and conditions to protect our rights, privacy, safety, or property, or those of other persons. Examples of bodies to whom we may voluntarily disclose data, in appropriate circumstances, include but are not limited to:
 - Third party service providers to facilities activities of SHIELD. Any transfer will be subject to an appropriate, formal agreement between NTU and the processor. An example of this is the agreement between NTU and GODaddy (the SHIELD App host).
 - Agencies with responsibilities for safeguarding minors where there are concerns about the safety and wellbeing of a child.
 - We might need to share or transfer your data confidentially with relevant parties and/or their professional advisers if there is a merger, acquisition, change of control, joint venture or other similar arrangement involving SHIELD.
 - Exceptionally we might need to share your personal information in order to obtain necessary confidential legal advice or to comply with insurance, legal or regulatory obligations.

How long we keep your data for

We will not store your personal information for longer than is necessary. NTU will ensure that our trusted partners and selected third parties with whom we share your personal information in accordance with this Privacy Notice will delete your personal information when they no longer require it.

In determining data retention periods, NTU takes into consideration local laws, contractual obligations, and the expectations and requirements of our data subjects. *SHIELD* also takes into consideration regulatory and best practice requirements. When we no longer need personal information, we securely delete or destroy it.

We intend to destroy copies of pdf reports generated by the SHIELD app, where these are provided to us, after holding them for 1 year. Contact, statistical and evaluation data will be held for 7 years following the end of your participation with SHIELD.

Anonymised information is not subject to a fixed retention period, as it cannot be traced back to an individual.

We may be obliged to suspend any planned destruction or deletion under our retention policy where legal or regulatory proceedings require it or where proceedings are underway such as require the data to be retained until those proceedings have finished.

How we secure your data

We have appropriate security measures in place to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business requirement to know.

NTU takes data security seriously, and we use appropriate technologies and procedures to protect personal information.

For example:

- Policies and procedures – measures are in place to protect against accidental loss and unauthorised access, use, destruction, or disclosure of data.
- Business Continuity and Disaster Recovery strategies that is designed to safeguard the continuity of our service to our clients and to protect our people and assets.
- Appropriate restrictions on access to personal information.
- Monitoring and physical measures, to store and transfer data securely.
- Data Privacy Impact Assessments (DPIA) in accordance with legal requirements and our business policies.
- Periodic training on privacy, information security, and other related subjects for employees and contractors.
- Vendor risk management.
- Contracts and security reviews on third-party vendors and providers of services.

How we keep your data secure in other countries

Your personal information may be transferred by us or our trusted partners outside of the UK and the European Economic Area (the “EEA”) for example our cloud storage for the SHIELD app is currently in {Based in Germany.

NTU SHIELD has networks, databases, servers, systems, and support located throughout the world. NTU SHIELD collaborates with third parties such as cloud hosting services, suppliers, and technology support located around the world to serve the needs of NTU, workforce, and students. Your personal information may be shared with record matching and customer targeting partners, including Google, Facebook, Snapchat and LinkedIn. Some of these partners process personal data in Canada and the United States of America.

In some cases, we may need to disclose or transfer your personal information within NTU SHIELD or to third parties in areas outside of the UK. The areas in which these recipients are located will vary from time to time, but may include the United States, Europe, Canada, Asia, Australia, India, and other countries.

We take appropriate steps to ensure that personal information is processed, secured, and transferred according to applicable law. When we transfer personal information from the UK to other countries in which applicable laws do not offer the same level of data privacy

protection as in the UK, we take measures to provide an appropriate level of data privacy protection.

In other words, your rights and protection remain with your data, i.e. we use approved contractual clauses, multiparty data transfer agreements, intragroup agreements, and other measures designed to ensure that the recipients of your personal information protect it. If you would like to know more about our data transfer practices, please contact DPO@ntu.ac.uk

Your rights

We respect your right to access and control your information, and we will respond to requests for information and, where applicable, will correct, amend, or delete your personal information.

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to ask us to correct any incomplete or inaccurate information we hold about you.
- **Request erasure** of your personal information in limited circumstances. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are processing your personal information on the basis of our legitimate interest (or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction or suspension of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Object to any direct marketing** (for example, email marketing or phone calls) by us, and to require us to stop such marketing.
- **Object to any automated decision-making** about you which produces legal effects or otherwise significantly affects you.
- **Request the transfer** of your personal information to another party.

How to contact us

If you are concerned about any aspect of the service we provide to you, you can use our complaints procedure. Please contact shield@ntu.ac.uk asking for the complaints procedure in the subject header. The procedure enables investigation of the concerns with the aim of satisfactory resolution as quickly as possible.

Please contact our [Data Protection Officer](#) with any requests related to your personal information.

If you are not satisfied with how we manage your personal data, you also have the right to make a complaint to a data protection regulator. The ICO contact details are: <https://ico.org.uk/global/contact-us/>

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes.

[Return to SHIELD website](#)