NRCPD Privacy Notice and Data Protection Policy

1. Introduction

This is the Data Protection Policy of NRCPD in force from 3rd February 2020. We keep our policies concerning data protection regularly updated in order to ensure compliance with the law and best practice in this area. Please note that we may therefore alter or replace this Data Protection Policy from time to time.

The privacy and security of personal information that we hold about those on our registers, our staff and Trustees, and professionals that support us in our work is paramount. NRCPD is committed to be an effective custodian of personal information, handling it responsibly and within the law, and securing it with industry standard administrative, technical and physical safeguards.

We follow two guiding principles when it comes to your privacy:

- **transparency** - we will tell people what information we hold about them, how we hold it and what we use it for.
- **accountability** - we are responsible for the personal information we hold and will be clear on the legal basis for which we hold it.

About us

The National Registers of Communication Professionals working with Deaf and Deafblind People (NRCPD) is registered as a data controller with the Information Commissioner's Office (ICO) (registered number ZA231154).

It is also a company limited by guarantee registered in England and Wales (company number 10510695), registered address NRCPD, Richard Annand VC House, Mandale Business Park, Belmont, Durham DH1 1TH.

NRCPD is a charity registered in England and Wales (registered charity number 1170904).

If you have any queries about data protection in NRCPD please contact us via enquiries@nrcpd.org.uk.

We'll update this Data protection Policy regularly to ensure it continues to comply with the latest regulations and best practice.

2. How we use your information

a) Storage and management of personal information

Our principal registration data management system is a bespoke CRM system which is maintained and developed by our principal information systems partner Transcendit Ltd. This system enables us to efficiently store the registers, and information about the registered professionals on them, including former registrants and trainees, in a way

that ensures adequate security and only allows people who have the right level of authority to access personal information. It also simplifies our responsibilities for data retention and subject access requests.

The system is cloud based and hosted on a GDPR compliant platform, Heroku. Access to the data is via an integrated portal. The Portal enables those on our registers to securely interact with their registration information; for the public to securely check registration and search for information on professionals; and helps NRCPD to securely manage changes to the registers as registration events occur.

b) Visitors to our website and social media platforms

We may collect and analyse information about visits to our website and portal to find out how people use the site and ways to improve it. This information is only processed in a way that does not identify anyone. We do not make any attempt to find out the identities of those visiting our website.

Like most websites we use cookies to help the site work more efficiently.

No user-specific data is collected by us or any third party. If you fill in a form on our website, that data will be temporarily stored on the web host before being sent to us.

When non-registered people are applying to join a register for the first time, we will hold information relating to that application prior to the registration being approved. If the application is not completed, or not approved we will only hold the information for a reasonable time and at the most 3 months.

NRCPD has a presence on various social media platforms. We will not collect or store any personal data from engagement with us via these platforms, however we are not responsible for how such third party services use your data. Currently we have a corporate presence on Facebook, LinkedIn, Instagram and Twitter. To find out about how these companies use your data and how you can control the way they use your data follow these links: Facebook; LinkedIn; Instagram; Twitter.

c) Registrants and Trainees – current and former

The lawful basis we use for processing current and former registrant's and regulated trainees' personal information is a combination of contract and legitimate interest. Initial registration and subsequent renewal is conditional on professionals giving consent for their personal information to be stored and processed (the contract element) so that NRCPD can fulfil its public benefit and charitable purpose of protecting the public by maintaining the registers (the legitimate interest element). NRCPD asserts the legitimate interest to retain personal information beyond the registration period for public protection in order to maintain a record of professional competence to practise, or restrictions on such practise that may have been applied. This includes where professionals are no longer on our registers irrespective of whether consent has been given or specifically withdrawn.

We carefully safeguard the information we hold about people who are or have been on our registers. This information comes from information provided through applications

and renewals, CPD records including audit findings, or any involvement in our professional conduct complaints process (as complainant, witness or respondent).

The information may also come from registrant's interactions with us, for example, through social media, website usage or surveys. It may include, for example, contact details, interests or guidance documents downloaded from our website (but as above we will not attempt to identify any individual from anonymous interactions online).

In addition, and on a voluntary basis we may collect equality monitoring information from current registrants at first registration and at renewal. Any such collection is optional for registrants and is not a condition of registration. The information we gather is in line with equality monitoring data used by organisations with a public function across the UK and helps us meet our obligations to ensure we do not unlawfully discriminate. The information is held separately from personal information and is only used anonymously and in aggregate to provide an understanding of the demographic of those we regulate.

d) What the personal information we hold is used for

We primarily collect personal information to fulfil our purpose of protecting the public by regulating communication professionals.

- The public can search on our website by name for a professional they may be working with, to check whether they are registered with us and whether their registration and any restriction on practise is appropriate for the assignment. The check can also be used to see the registration status of anyone about whose practise they may wish to raise a concern or complaint.
- If a practise restriction is imposed on a professional their entry will be endorsed accordingly, and this will be publicly visible if searched. This includes suspension.
- Where someone is found not to be safe to practise and is removed from the register (via a Complaint Committee finding), that decision is published on the website with the individual's name, and they do not appear in search results.
- Professionals no longer on our registers (ie who by choice have not renewed) will not come up in any website search and this means that NRCPD can no longer provide any assurance as to their professional competence.
- Past registration information is retained so that we can maintain a continuous record of professional competence should someone wish to re-join the registers or if we need to access the information for some other legitimate regulatory reason.
- We will retain personal information relating to any registrant involved in a complaint for at least 6 years.

We offer a facility on our website for members of the public to search for professionals to work with in their area. Information about a person will only be displayed in this search if they have opted in and they can choose which information they wish to be displayed. They can change or opt out of this at any time.

We will also use collective registration information to support our understanding of the demographic, national distribution and development of the professions and which we

may share with other organisations at our discretion in furthering our charitable objects. This will be to manage NRCPD operations and for our work with others to further the interests of 'healthy professions' that meet appropriate standards for public protection. We will never allow individuals to be identified when we use information in this way.

We may also use personal information for identity verification - when registrants call us, we may need to do this depending on the nature of the enquiry. We may do this by asking for certain information known only to them.

Additionally, we may use registrant information to:

- carry out regulatory checks and meet our obligations as a regulator
- develop and improve our services
- improve the relevance of information messages we may send you
- personalise our website for you
- protect our systems

We may also monitor, record or take a written record of any communications with registrants including telephone calls. We'll use these records to track mutual undertakings, to analyse, assess and improve our services and for training and quality purposes.

We send messages by post, telephone, text, email and other digital methods. These messages may be:

- to help you manage your registration
- to meet our obligations, for example inspections and visits by Regulators eg the Charity Commission
- to carry out any of NRCPD's regulatory functions
- to keep you informed about the features and benefits of NRCPD registration and services and other matters that may be of professional interest to you.

We will never pass on your information to a third party to use in their own direct marketing without your specific consent. In carefully considered circumstances we may however pass information to you on behalf of a third party if it is broadly in the interests of regulation and the professions.

Any equality monitoring information provided by you is treated separately from all the above, is not identifiable to you and is never released to any other party other than in aggregate as part of our normal business operations.

e) Sharing your information

During your contact with us, we'll tell you how your information will be used and if it may be necessary to share it with other organisations.

We will not share personal information with any third parties unless:

- you have consented to this (for example by providing information to us after we've told you that we will supply the information to a third party)
- you have opted to be visible in search results when the public are looking for professionals to work with
- it is required for the management of your registration or a legitimate business purpose (for example accounting services).
- it is part of our duty to protect a child, a vulnerable adult, yourself or the public
- for the prevention and detection of crime or the assessment of any tax or duty
- we are required to do so by any court or law or any relevant regulatory authority acting within the law
- to protect the rights, property or safety of NRCPD or any third parties (for example for the purposes of fraud protection)
- we transfer our rights and duties to provide products and services to another organisation.

As an independent regulator, it is in our legitimate interests to verify the registration status of an individual when we receive a query from a third party, including registration details and expiry dates. We do this via the search facility on our website but will also do so if we receive the query in any other form.

We will provide certificates of registration as evidence of an individual's CPD and periods of registration with us when asked by other regulatory bodies.

By registering with NRCPD, registrants and regulated trainees give consent to us to process personal data which they have provided to us.

One significant role of NRCPD is to promote the registrations and qualifications of our registrants and trainees to the public. To this end we offer a searchable register directory on our website and we answer telephone queries where we will refer callers the search facility. Inclusion is voluntary and registrants opt into or out of this service or from certain information being included. Information displayed is: current registration status; date they first registered; the expiry date of registration; current register category; relevant qualifications, preferred working hours, contact details and supplementary information added by the registrant to assist the public. This information may be used by others to contact you to work but NRCPD is not responsible for the reasons people have for seeking your details in this way.

When you make online card payments to us, we use a third party processor, Stripe, to manage the process and the payments.

We will keep records of payments for financial audit reasons for six years. The basic records of a registrant or regulated trainee's name and registration period will be kept for a reasonable period of at least 6 years in case ex-members wish to re-join. We'll also keep records of qualifications, complaints and adjudications for six years unless there is a legitimate reason to keep it for longer.

When people make complaints against registrants, we hold data relating to the complainant as well as details of the complaint and witnesses or interested parties. We share information with case examiners, legal advisers, committee members and external clerks who all sign data processor and confidentiality agreements with us. All

data relating to this process is kept very securely. Paper records are kept on-site in secure cabinets with limited access, may be archived securely off-site one year after case closure, and destroyed 6 years after case closure, unless there is a legitimate reason for not doing so. If for any legitimate regulatory or lawful purpose case material is reused in another case then the retention period for that material relates to dates for the later case.

f) Sharing Information with Other Regulators

In order to fulfil our regulatory purpose and protect the public we assert a legitimate interest in sharing information with other regulators about complaints decisions resulting in practise restrictions, suspensions and register removals in order to ensure that respective professionals are unable to evade practise sanctions by registering with other bodies. This may include proactively sharing information where decisions and sanctions are new. We will not share the case materials for this purpose unless there is an overriding legitimate interest within the law.

g) Approval of qualifications as routes to registration

From time to time we approve qualifications as routes to registration. We do this by mapping the respective qualification against the agreed standard (for example the National Occupational Standards for Interpreting).

We use professional standards advisers and assessors to do this. We have data processor agreements with them. Once an approval decision is made, the information and report on the mapping is retained by NRCPD for as long as the qualification remains unchanged and for three years thereafter. If the qualification changes (whether or not as a result of a change in the relevant standard) the course will be mapped again.

We will publish our approval decision without giving detailed reasons by saying that a qualification is or is not approved as a route to registration. The awarding body in question will always be informed of full reasons for any decision.

h) CPD audit

CPD audit is managed internally with data stored on our CRM and on spreadsheets. Any hardcopy materials that are sent in or produced are stored in secure cabinets and securely destroyed once the audit is complete.

i) Members of the public who make enquiries

We may record information from members of the public who contact us with general enquiries. We will record the information provided in our CRM database and in our email system.

j) Job applicants, current and former staff

We will only use information you provide during the recruitment process to progress your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any information you provide during the process with any third parties for marketing purposes or store it outside of the European Economic Area. The information you provide will be held securely by us or our data processors, whether the information is in electronic or physical format.

We advertise roles with Indeed, Deaf Jobs UK and other online job services. We use Indeed to help us manage applications and find the right candidates through their online portal. For how Indeed process your information please go here https://www.indeed.co.uk/legal.

We will use the contact details you provide to progress your application. We will use the other information you provide to assess suitability for the role you've applied for.

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for, but it might affect your application if you don't.

If we make a conditional offer of employment, we'll ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff and their right to work in the UK, and to seek assurance as to their trustworthiness, integrity and reliability.

Therefore, you must provide:

- proof of your identity – we'll ask you for original documents and will take copies for verification purposes.
- proof of your qualifications – we may ask you for original documents and will take copies for verification purposes.

We will contact your referees directly to obtain references using the details you provide in your application.

If we make a final offer, we'll also ask you for the following:

- bank details – to process salary payments
- emergency contact details – so we know who to contact if you have an emergency at work
- Medical information so that you can be safe in the workplace
- Equality data so that we can monitor our diversity performance

If you accept a final offer from us, some of your personnel records will be held on our HR records system.

During your employment we may need to share your information with third party processors who provide elements of our ongoing employment service, that is employment law advice, occupational health advice, payroll and pensions processing and other employee benefits such as health and wellbeing services. We have

contracts in place with all of our third party processors. This means they cannot do anything with your personal information unless we instruct them to do so. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

If you are employed by us you will be auto-enrolled into the People's Pension, unless you opt out, and relevant details about you will be provided to B&CE Holdings who administer the scheme. Details include your name, date of birth, National Insurance number and salary.

The information you provide will be retained as part of your employee file for the duration of your employment and for six years afterwards.

If you're unsuccessful, the information you give us, and any information we create during the process, is retained for six months.

k) People who visit our premises

We record the name of all visitors to our offices for safety and security reasons. This information is deleted after three months.

l) People who take part in our surveys and consultations

We use third party processors for both our internal and external surveys. We collect minimal personal data in surveys - generally only IP address or similar so that we can uniquely identify responses. We keep information only for the duration of the survey campaign. The survey will normally allow anonymous responses – if it does not this will be made clear. If you are asked to provide contact details such as email this will be on a voluntary basis.

3. Special Categories of Personal Data

What we mean by special categories of personal data is data relating to any data subject which reveals:

- Racial or ethnic origin.
- Political opinions.
- Religious and philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Sex life and sexual orientation.

It is not our policy to collect data that falls into these special classes of personal data save where to do so is necessary for us to comply with the law or properly to discharge our obligations or functions as an organisation. In certain circumstances therefore we may need to process such data. When that need arises, we will only process that data in accordance with the law. Where required to do so by law we will advise any data subject concerned of all relevant details in connection with the

processing. We will also, where required to do so, advise any data subject concerned of the specific purpose(s) for which we are processing that data and seek their explicit consent to the processing before such processing takes place, and in such cases we will only process such data in accordance with such explicit consent when the same is freely given.

4. Audit and regulatory requirements

We may share any data about our operations with:

- our auditors, RSM UK LLP
- HMRC
- the Charity Commission
- the Information Commissioner's Office
- Companies House

and others by whom NRCPD is regulated, should this be necessary to complete our statutory audit and regulatory requirements.

We use two law firms to provide advice and guidance on a range of topics and we may share personal data with them at times. Lupton Fawcett provide us with advice relating to corporate, commercial and charity law and other general areas of legal concern – we do not provide them with any person identifiable information relating to registrants and trainees. Kingsley-Napley provide us with advice and support for our professional complaints process and as such are in a position of legal privilege to receive and process personal information in relation to any individual involved in a complaint in order that NRCPD can fulfil its regulatory purpose. A confidentiality agreement covers their processing of such data. All third parties have contracts with us which includes a third-party processor agreement.

5. Your rights

Under the General Data Protection Regulation (GDPR) you have rights as an individual data subject which you can exercise in relation to the information we hold about you. You can read more about these rights on the ICO's website.

6. Complaints and queries regarding the processing of information

We try to meet the highest standards when collecting and using personal information, and we take any complaints about this very seriously. We encourage you to let us know if you think that our collection or use of information is unfair, misleading or inappropriate. We also welcome any suggestions for improving our procedures.

This privacy notice does not provide exhaustive details of all aspects of our collection and use of personal information. However, we're happy to provide any additional information or explanation needed. Please send any requests to the address in the **Introduction** above.

If you want to make a complaint about the way we've processed your personal information, you can contact the ICO as the statutory body which oversees data protection law - see ICO concerns.

7. Access to your personal information

We try to be as open as we can in terms of giving people access to their personal information. You can find out if we hold any personal information about you by making a ‘data subject access request' (DSAR) under GDPR.

Once we receive a DSAR, we will process it in line with the law and ICO guidelines to:

- give you a description of it
- tell you why we are holding it
- tell you who it could be disclosed to
- let you have the information we are required to provide in an intelligible form.

To make a DSAR you should write to us at the address in the **Introduction** above.

If you agree, we'll try to deal with your request informally, for example by providing you with the specific information you need over the telephone.

You can ask us to correct any mistakes in any information we hold.

The GDPR also gives you the right to have the data we hold about you deleted in some circumstances. This is called the 'right to erasure'. It does not apply to all data but applies in the following circumstances:

- We no longer need your data
- You originally provided consent and have now withdrawn this unless we retain a legitimate interest in that data.
- You have objected to the use of your data and your interests outweigh ours within the law.
- We have collected your data unlawfully
- We have a legal obligation to erase your data.

If you would like to exercise your right to erasure, please get in touch.

8. Disclosure of personal information

Generally, we will not disclose personal data without consent. However, we may do so when compelled by a legal authority to do so for example for the investigation of a crime or by another regulatory body, or for our own purposes in collecting evidence in relation to a complaint.

9. Data security

We recognise that the information you provide may be sensitive and we will respect your privacy. We keep information about you confidential. This means we store it securely and control who has access to it. We sometimes share personal data with

third parties where we have contracted them to carry out specific tasks for us. In such cases we carefully select which partners we work with. We take great care to ensure that we have a contract with the third party that states what they are allowed to do with the data we share with them. We ensure that they do not use your information in any way other than the task for which they have been contracted.

We will only share personal data with other organisations where we are satisfied that the other organisation is entitled to receive it and will keep your information secure.

We're committed to holding all personal data within NRCPD on secure systems. We keep any paper-based personal data in locked cabinets to which only appropriate staff have access. We're working to reduce the amount of paper-based information we hold as it is easier to secure data if it is only held electronically. The majority of personal data is held electronically on our CRM system that is maintained by Transcendit and hosted on Heroku. From time to time personal information is also held and transmitted within Office365 provided and hosted by Microsoft.

We use third party processors to provide email spam monitoring and filtering.

We have invested extensively in ensuring our information systems are secure and that our staff are suitably trained.