APPLICANT AND EMPLOYEE PRIVACY NOTICE

The Challenge Network (The Challenge) is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you prior to, during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR) or any subsequent data protection legislation in force from time-to-time.

The Challenge is a "Data Controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former job applicants and employees. This notice does not form a fixed part of your contract of employment or any other contract to provide services so we may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

DATA PROTECTION PRINCIPLES

We will comply with data protection law and ensure that the personal information we hold about you is:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

THE KIND OF INFORMATION WE HOLD ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which requires a higher level of protection.

We will collect, store, and use the following categories of personal information and ‘special categories’ of personal information about you:

- contact details;

- diversity information (including ethnicity and religion);
- gender;
- date of birth;
- medical and safeguarding information;
- right to work information;
- recruitment information (including CV, reference checks and next of kin);
- safeguarding information (including any criminal convictions and offences);
- performance management records;
- financial information (including bank details and National Insurance number);
- information about your use of our systems;
- driving licence and insurance information (if driving for work); and
- marketing and evaluation material (which includes videos, photos, recordings, testimonials and quotes).

HOW IS YOUR PERSONAL INFORMATION COLLECTED

We collect personal information about you through the application and recruitment process, either directly from you or sometimes from an employment agency, former employers or background check providers such as GB Group.

We will collect additional personal information throughout any recruitment process and subsequent period of you working for us to the extent necessary to monitor and evaluate your performance and ensure your compliance with our policies and procedures.

HOW WE WILL USE INFORMATION ABOUT YOU

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- where we need to perform the contract we have entered into with you;
- where we need to comply with a legal obligation including where it is necessary to cary out obligaions or exercies rights related to your employment;
- where it is necessary for our legitimate interest (or those of a third party); and

- we may also use your personal information in the following situations, which are likely to be rare:
    - where we need to protect your vital interests; and
    - where it is needed in the public interest.

Situations in Which We Will Use Your Personal Information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

The situations in which we will process your information are listed below.

- making a decision about your recruitment, appointment or continued employment;
- assessing qualifications for a particular job or task, including decisions about promotions;
- checking you are legally entitled to work in the UK;
- to ensure you are safe and supported whilst on the programme and allow us to comply with our legal obligations to keep young people safe;
- paying you and, if you are an employee, deducting tax, and making both National Insurance and pension contributions;
- administering the contract we have entered into with you;
- conducting performance reviews, managing performance and determining performance requirements;
- gathering evidence for possible grievance or disciplinary hearings;
- education, training and development requirements;
- dealing with legal disputes;.
- ascertaining fitness for work;
- managing sickness absence;
- complying with health and safety obligations;

- to prevent fraud;
- to monitor your use of our information and communication systems to ensure compliance with our IT policies;
- evaluating your experience of working at The Challenge;
- to ensure you have a driving licence and appropriate insurance (if driving for work;
- to ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution; and
- equal opportunities monitoring.

If You Fail to Provide Personal Information

If you fail to provide personal information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we not be able to continue to employ you e.g. if doing so would prevent us from complying with our legal obligations (such as to ensure the health and safety of the young people or check your right to work).

Change of Purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

HOW WE USE PARTICULARLY SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We have in place an appropriate policy document and safeguards, which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations or exercise rights in connection with employment.

- Where it is needed in the public interest, such as for equal opportunities monitoring

We may also process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences to determine your suitability for the role.

We are allowed to use your personal information in this way to carry out our obligations to protect and safeguard the vital interests of the young people who take

part in our programme.

DATA SHARING

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. In limited circumstances, we may transfer your personal information outside the EEA. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-parties may receive my personal information?

"Third parties" includes funders, partners, service providers, contractors and designated agents. The following third-parties may, depending on your job role, also process personal information about you:

- the NCS Trust CIC, if your work involves delivery of the NCS programme and only to the extent that they have a legitimate interest, legal obligation or other legal bases for receiving that information as Data Controller in their own right. NCS Trust explain what kind of information we share, what they do with it and other key information in their privacy policy at http://www.ncsyes.co.uk/privacy-policy.

- the Department for Education, the Education Skills Funding Agency or any other funding body connected with the programme you work on which has a have a legitimate interest, legal obligation or other legal bases for receiving that information as Data Controller in their own right;

- Inspira (if you work on the NCS programme in the Lancashire region);

- regulatory authorities; and

- those who provide products or services to The Challenge (such as payroll administrators, local delivery partners, insurers, office management companies, activity centres, IT platforms and Disclosure and Barring Service providers).

Which third-party service providers process my personal information?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes

and in accordance with our instructions.

We may share your personal information with other third parties, for example with a regulator or to otherwise comply with the law.

Transferring information outside the EEA

We may from time to time to use the services of an IT provider that stores or accesses your personal information outside the European Economic Area (EEA). However, we will only do so if there are appropriate safeguards in place to protect the information. For example, we will put in place European Commission model contractual clauses, ensure the supplier has binding corporate rules in place regarding data security and/or ensure the European Commission recognises the relevant country as having adequate data security.

DATA SECURITY

We have put in place appropriate security measures to prevent your personal information 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 need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

DATA RETENTION

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are as follows:

Subsection	Record Type	Format	Retention Period and Deletion or Disposal Deadline
i.	Job applications and interview records of unsuccessful candidates	Paper	6 months after notifying unsuccessful candidates (or longer, if there is a clearly communicated policy to keep candidates CVs for future reference). Application forms should give applicants the opportunity to object to their details being retained.
ii.		Electronic	
iii.	Next of kin or beneficiaries forms	Electronic	Once employment ends or 6 years after any payment of benefits.
iv.	Bank Details held by HR or Staffing	Electronic	Core Staff - 3 months from the date the employment ends. Seasonal Staff – 6 months from

Subsection	Record Type	Format	Retention Period and Deletion or Disposal Deadline
			the data the employment ends.
v.	Fit Notes	Electronic	1 year from receipt of the note.
vi.	Right to Work documents	Electronic	2 years from the date the employment ends.
vii.	Working time opt-out forms	Electronic	2 years from the date on which they were entered into.
viii.	Records to show compliance with the Working Time Regulations 1998	Paper or Electronic	2 years after the end of the relevant working time period that the record relates to.
ix.	Maternity records paternity records and shared parental leave records	Electronic	3 years after the end of the tax year in which the payment period ended.
x.	Accidents at work	Electronic	3 years from the date the report was made. If on NCS Programmes follow Incident deadline if accident qualifies as an Incident.
xi.	Risk assessments	Electronic	3 years from the date of the risk assessment.
xii.	Records in relation to hours worked and payments made to employee	Electronic	3 years from the end of the pay reference period to which the payments relate.
xiii.	Contact details, employment and volunteering contracts, variations, training records, performance records, absence dates and reasons, salary records, driving licence and insurance related documents, pension schemes information (including accounts and actuarial valuation reports) and other employment relation documents inc. flexible working, disciplinary, complaints	Electronic	6 years from the date the employment or volunteering ends.
xiv.	Disclosure and Barring Service (DBS) certificate and disclosures of criminal records forms	Electronic	Delete all certificates and any irrelevant or spent disclosures as soon as checked and only retain a copy where necessary for validation/dispute and even then for longer than 6 months after receipt.
xv.	Disclosure and Barring Service (DBS) note whether certificate was satisfactory or unsatisfactory (not copy) plus disclosures of relevant and unspent criminal records	Electronic	6 years after employment ends subject to xvi and xvii.
xvi.	Details of any safeguarding allegations against a member of staff relating to a young person and any personal data or special category data related to that Incident	Electronic	20 years after the allegation is notified to the Challenge or until the member of staff has reached normal retirement age, whichever is the later.
xvii.	Incident Information and any personal data or special category data related to that Incident	Electronic (and scanned paper copies)	20 years from the date of the Incident or alleged Incident (whichever is the later). Incident levels are defined in our Major

Subsection	Record Type	Format	Retention Period and Deletion or Disposal Deadline
			Incident Procedures and Crisis Comms Plan.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee of The Challenge we will retain and securely destroy your personal information in accordance with our data retention policy.

RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION

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 during your working relationship with us.

Your rights in connection with 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 have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. 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 relying on a legitimate interest (or those 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 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.

- **Request the transfer** of your personal information to another party.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

RIGHT TO WITHDRAW CONSENT

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer at dpo@the-challenge.org. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

OTHER REQUESTS / ISSUES

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information or if you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Last updated 24/05/18