



York Community Consulting

Privacy Policy

Last Updated: 10 DECEMBER 2025

Table of Contents

Summary of Key Points	4
1. What information do we collect?	5
1.1 Applicants and Account Holders	5
1.1.1 Sensitive Personal Information	5
1.2 Clients	5
1.3 External Mentors	5
1.4 Information Automatically Collected	6
1.5 Information Collected from Other Sources	6
2. How do we process your information?	6
2.1 Applicants and Account Holders	7
2.1.1 Sensitive Personal Information	7
2.2 Clients	8
2.3 External Mentors	8
2.4 Information Automatically Collected	8
2.5 Information Collected from Other Sources	9
3. When and with whom do we share your personal information?	9
4. How long do we keep your information?	10
4.1 Applicants and Account Holders	11
4.2 Clients	11
4.3 External Mentors	11
4.4 Information Automatically Collected	11
4.5 Information Collected from Other Sources	12
5. How do we keep your information safe?	12
5.1 How do we store your information?	12
5.2 International Data Transfers	12
6. Do we collect information from minors?	13
7. What are your privacy rights?	13
7.1 Right to Access	13
7.2 Right to Rectification	13
7.3 Right to Erasure	14
7.4 Right to Restrict Processing	14
7.5 Right to Data Portability	14
7.6 Right to Object	14
7.7 Rights related to Automated Decision Making and Profiling	14
7.8 Withdrawing your Consent	14
7.9 Opting Out of Marketing and Promotional Communications	14
7.10 Account Information	15
7.11 How to Exercise Your Rights	15

7.11.1 Filing a Complaint	15
8. Do Not Track Browser Controls	15
9. Do we make updates to this policy?	16
10. How can you contact us?	16

This Privacy Policy for York Community Consulting (“York Community Consulting”, “YCC”, “we”, “our”, or “us”), describes how and why we collect, store, use, and/or share (“process”) your information when you use our services (“Services”), such as when you:

- Visit our website at <https://www.yorkcommunityconsulting.co.uk> (“Website”), or any website of ours that links to this Privacy Policy
- Create an account and submit an application through our Website Portal
- Engage with us as a client or consulting partner
- Engage with us in other related ways, including events, marketing communications, or employment verification requests

Data Controller

The Data Controller for your information is the York Community Consulting Committee. Use the contact details in [Section 10](#) to get in touch.

Questions or Concerns?

Reading this Privacy Policy will help you understand your rights and choices regarding your information. If you do not agree with our policies and practices, please do not use our Services.

If you still have any questions or concerns, please [contact us](#).

Summary of Key Points

This summary highlights key points from our Privacy Policy and does not replace the full policy. You can find more detailed explanations and legally binding terms in the sections that follow.

What personal information do we process? When you visit, use, or navigate our Services, we may process personal information depending on how you interact with us, the choices you make, and the features you use.

Do we process any sensitive personal information? Yes - we process diversity and inclusion data only through optional voluntary submission.

Do we receive any information from third parties? We may receive information from public databases, social media platforms, and event partners.

How do we process your personal information? We process your information to operate, improve and administer our Services; communicate with you; ensure security; and comply with legal obligations.

Do we share personal information? We may share information in specific situations with specific third parties as outlined in [Section 3](#).

How do we keep your information safe? We use organisational and technical measures to protect your information, though no system is perfectly secure.

What are your rights? Depending on where you live, you may have certain rights regarding your personal information.

1. What information do we collect?

The information we collect depends on how you interact with our Services.

1.1 Applicants and Account Holders

When you create an account and submit an application through our portal, we collect:

- Contact details (e.g., name, email address, and password)
- Education details (e.g., level of study, start and end dates, and degree course)
- Application details (e.g., CV, vacancy preferences, and responses to application questions)

1.1.1 Sensitive Personal Information

We collect the following sensitive personal information only if you voluntarily choose to provide it:

- Gender, sexual orientation, and ethnicity

These questions are optional, and you may select “Prefer not to say”. Further details on how we use and store this data can be found in [Section 2.1.1](#).

1.2 Clients

We only collect the information necessary to deliver consulting services:

- Organisation name, address, and industry
- Contact information of staff (including name, email address, and phone number)
- Project specifications, deliverables, and timelines
- Project communication and documentation, and other related project data

1.3 External Mentors

We only collect the information necessary for collaboration:

- Name and email address

We do not collect additional personal information unless necessary or legally required.

1.4 Information Automatically Collected

When you visit, use, or navigate our Services, we may automatically collect certain technical information from your device. This data may be personal data where it could be used to identify you (for example, when linked with your account or other information), and may include:

- IP address and approximate location
- Browser type and version
- Device type, operating system, and language preferences
- Dates, times, and pages accessed
- Referring and exit URLs
- Interaction data such as clicks, scroll events, and time spent on pages
- Session recordings and heatmaps collected through our analytics provider

For more information on cookies, tracking technologies, and how you can manage your preferences please see our [Cookie Policy](#) for full details on consent and controls.

1.5 Information Collected from Other Sources

We may occasionally collect limited information about you from publicly available or third-party sources to maintain the accuracy of our records and communications. These sources may include:

- Public databases
- Social media platforms
- Event or recruitment partners

The information obtained may include contact details such as name, email address, organisation or professional role. See [Section 2.5](#) for how we process this information.

2. How do we process your information?

We process your information to provide, improve, and administer our Services, communicate with you, for security and fraud prevention, and to comply with the law. We may also process your information for other purposes with your consent.

Under UK GDPR legislation, we must have a valid lawful basis each time we process your personal data. In this section we explain our lawful basis for each type of processing. In summary, we generally rely on:

- Article 6(1)(b) Contract Performance - where we need to process your data to enter into or perform a contract with you (for example, to process your application or deliver consulting services to clients).
- Article 6(1)(f) Legitimate Interests - where the processing is necessary for our legitimate interests or those of a third party, provided these are not overridden by your rights and freedoms (for example, to keep our Services secure, maintain records, improve how we run projects, or communicate with mentors).
- Article 6(1)(a) Consent - where you choose to opt in to certain optional activities, such as non-essential analytics tools (including session recordings), and you can withdraw this consent at any time without affecting the lawfulness of processing before withdrawal.

For the limited special category data we collect voluntarily (diversity and inclusion information), we also rely on an additional condition in Article 9(2)(j) of UK GDPR for archiving, research and statistics, together with relevant safeguards under the Data Protection Act 2018 (as explained in Section 2.1.1).

The specific bases and purposes for each activity are detailed in the subsections below.

2.1 Applicants and Account Holders

We use the personal information you provide to:

- Facilitate account creation, management, and authentication
- Process and evaluate any applications you submit
- Communicate with you regarding your account status and application progress
- Maintain records for compliance, audit, and reporting purposes
- Improve our Services and user experience through feedback and usage analysis

We process this information based on the following legal grounds:

- Article 6(1)(b) of UK GDPR: Contract Performance
- Article 6(1)(f) of UK GDPR: Legitimate Interests

2.1.1 Sensitive Personal Information

We collect optional diversity and inclusion information to monitor and improve the fairness and inclusivity of our recruitment process. Providing this information is entirely optional and will not affect your application. As such, you may select “Prefer not to say” or leave the questions blank entirely.

When you submit a response, we immediately separate and anonymise it from your application data so they cannot be linked back to your identity or application, and we do not retain any keys or linkable identifiers that would enable re-identification. Once anonymised,

this information is no longer personal data and cannot be accessed or erased at an individual level.

Purpose Limitation. We use this data solely for aggregate-level analysis and reporting to foster diversity and equity.

Safeguards. We implement strong data protection measures including minimisation, anonymisation from collection, limited access to data, and clear transparency regarding processing.

Before anonymisation, we process this information based on the following legal grounds:

- Article 6(1)(f) of UK GDPR: Legitimate Interests
- Article 9(2)(j) of UK GDPR: Archiving, research and statistics (with safeguards under the Data Protection Act 2018 and our Appropriate Policy Document).

2.2 Clients

We process client information to:

- Deliver consulting services according to agreed terms
- Manage projects, timelines, and communicate with stakeholders
- Maintain necessary records for compliance, audit, and accountability
- Improve the quality and delivery of our Services

We process this information based on the following legal grounds:

- Article 6(1)(b) of UK GDPR: Contract Performance

2.3 External Mentors

We use External Mentors' contact details to:

- Communicate about project work and related activities
- Coordinate mentoring support for our project teams

We process this information based on the following legal grounds:

- Article 6(1)(f) of UK GDPR: Legitimate Interests

2.4 Information Automatically Collected

We collect technical and usage information automatically to:

- Maintain the security, stability, and performance of our Services (for example, server logs and basic diagnostic information)
- Detect and prevent fraud, abuse, and security incidents
- Understand usage trends and improve user experience

- Conduct internal analytics and reporting
- Collect session recordings and user interaction heatmaps via our analytics provider, but only after you provide explicit consent for these optional analytics tools.

We process this information based on the following legal grounds:

- Article 6(1)(a) of UK GDPR: Explicit Consent - for non-essential analytics (including session recordings and heatmaps) which only run if you choose to accept them through our cookie preference banner, and which you can withdraw at any time.
- Article 6(1)(f) of UK GDPR: Legitimate Interests - for essential logging and security-related processing that is necessary to keep our Services secure and functioning properly.

2.5 Information Collected from Other Sources

We may process data obtained about you from third-party or publicly available sources to:

- Keep our contact records accurate and up to date
- Follow up on specific expressions of interest in our Services or events

We process this information based on the following legal grounds:

- Article 6(1)(f) of UK GDPR: Legitimate Interests

3. When and with whom do we share your personal information?

We may share your information in the following circumstances, always ensuring your data remains protected and used only for legitimate purposes.

Business Transfers. If the structure of York Community Consulting changes (for example, we incorporate or merge with another organisation), we may transfer your information to the relevant third parties involved in such a transaction.

Legal Requirements. We may disclose your information to comply with laws, court orders, government requests, or to protect the legal rights, safety, and security of York Community Consulting, our users, or others.

Employment References. If you are a former applicant or employee, we may verify your employment upon request from a prospective or current employer, providing only limited details such as your name, role, and project involvement. We will take reasonable steps to verify the identity and legitimacy of the requester before sharing this information.

Employees. Depending on their role, different employees may access relevant personal and client data to perform their duties related to project oversight, administration, and service delivery. Access is role-based and governed by strict confidentiality policies.

External Mentors. Mentors involved in projects may access specific client data necessary for mentoring and supporting project teams. They are bound by confidentiality agreements and only access the minimum data necessary for their mentoring activities.

Service Providers. We share personal data with trusted third-party service providers to help us operate and improve our Services, including:

- Cloud hosting and infrastructure providers who store and process your data securely (for example, our website hosting provider)
- Email and communication service providers we use to send application updates and other messages
- Payment processors (if applicable) for managing transactions
- Analytics and security providers that help us understand Service usage and protect against fraud and abuse, in line with your consent and cookie preferences

We carefully select our service providers and use providers that are committed to data protection and GDPR compliance. Where they act as our data processors, we rely on appropriate contractual terms (for example, data processing agreements, standard contractual terms, or equivalent data protection wording in their standard terms) which require them to protect your information, keep it secure, and only process it on our documented instructions.

We do not sell your personal information. Any other sharing beyond the above will only occur with your explicit consent or as legally required.

More information about our cookies and similar technologies used by our analytics and security providers is set out in our [Cookie Policy](#).

4. How long do we keep your information?

We retain your information only for as long as it is needed to fulfil the purposes for which it was collected, or to comply with legal obligations. The retention period depends on the context of the processing and our legitimate business needs. Once we have no ongoing legitimate business need to process your information, we will either delete or anonymise such data.

Note if deletion is not currently possible (for example, because your personal information has been stored in backup archives), we will securely store your information and isolate it from any further processing until deletion is possible.

See below for specific retention periods per collection category.

4.1 Applicants and Account Holders

For Unsuccessful Applicants. We will retain your personal information for 6 months post rejection, after which your information will be permanently anonymised. This allows us to respond to any queries or legal claims relating to our recruitment process.

For Successful Applicants. We will retain your personal information while you are actively employed by us, and then for a further 3 months, after which your information will be permanently anonymised. This allows us to maintain accurate records of your engagement with us and respond to any queries or legal claims relating to your employment.

For Account Holders. We will retain your personal information for as long as your account remains active, and for up to 2 years after your last activity, after which it will be deleted or anonymised unless we need to keep it for legal or security reasons.

For Sensitive (Diversity and Inclusion) Data. Your data is immediately anonymised at the point of submission, and retained indefinitely for aggregate data analytic purposes.

For Employment Verification Data. We will retain minimal personal information for as long as we reasonably need to be able to respond to verification requests. This includes basic information such as your name, your position, and your department whilst employed.

4.2 Clients

We will retain your data, including project information and communications, for a period of up to 7 years after the completion of your project for legal, audit, and compliance purposes. After this period, your data will be permanently deleted.

4.3 External Mentors

We will retain your contact details for as long as you remain actively involved with our projects or mentoring activities. When you cease to be involved with our Services, we will retain your information for a period of up to 1 year before permanently deleting such data.

4.4 Information Automatically Collected

For Server Logs. Our Website hosting provider retains all log data for a maximum of 1 week before permanently deleting such data.

For Analytics Data. Our Analytics provider retains all data for a maximum of 1 year before permanently deleting such data. In cases of session recordings and user interaction heatmaps, this data is retained for a maximum of 30 days before being permanently deleted.

4.5 Information Collected from Other Sources

For Personal Information. We will retain your data under the same conditions as laid out in [Section 4.1](#).

For Newsletter Contact List Information. We will retain your data under the same conditions as laid out in [Section 4.1](#), or until you unsubscribe from such emails.

5. How do we keep your information safe?

We have implemented appropriate and reasonable technical and organisational security measures which are designed to protect the security of any information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the Internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that unauthorised third parties will not be able to defeat our security and improperly collect, access, steal, or modify your information.

Although we will do our best to protect your information, transmission of information to and from our Services is at your own risk. You should only access our Services within a secure environment.

5.1 How do we store your information?

All of your information is stored securely on encrypted servers hosted by our cloud service providers. Access to this information is restricted to authorised York Community Consulting employees on a need-to-know basis through role and time-based access controls, ensuring staff only have access to the data necessary to perform their specific role or function.

Our staff are trained on data protection and confidentiality practices to ensure they handle your information appropriately. We also regularly assess and evaluate the effectiveness of our security measures through regular reviews and testing.

5.2 International Data Transfers

Some of our Service Providers are based outside of the UK, or use sub-processors outside of the UK (for example, global cloud infrastructure providers). Where this involves a transfer of personal data to a country without UK adequacy regulations, we rely on appropriate safeguards such as the UK International Data Transfer Addendum to the EU Standard

Contractual Clauses, or, where the provider is certified, the UK extension to the EU-US Data Privacy Framework.

Where possible, we choose UK or EU data centre regions, but providers may still have limited access arrangements from other countries. In all cases, our providers are required to protect personal data to UK GDPR standards.

You can [contact us](#) if you would like more information about the specific safeguards we use for international transfers, or to request a copy of standard clauses where legally permissible.

6. Do we collect information from minors?

Most users of our Services are adults aged 18 and over. We do not knowingly solicit data from or market to children under 18 years of age.

By using these Services, you represent that you are at least 18 years old or that you are the parent or guardian of a minor and consent to such minor's use of our Services.

If you become aware of any data we may have collected from minors in violation of this policy, please [contact us](#). We will review the situation and, where we do not have appropriate consent or another valid lawful basis to keep the data, we will delete it unless we are legally required to keep it.

7. What are your privacy rights?

You have certain rights regarding the information we hold about you. These rights help you control how your data is used and ensure we process it fairly and transparently. Some rights only apply in certain situations, depending on the lawful basis we are relying on and the type of processing we are carrying out.

7.1 Right to Access

You have the right to request access to the information we hold about you, including details about how we process and share your data.

7.2 Right to Rectification

If your information is inaccurate or incomplete, you have the right to ask us to correct or complete it.

7.3 Right to Erasure

You can request the deletion of your data in certain cases, such as when it is no longer needed or if you withdraw consent. However, some data may be retained to comply with our legal obligations or for legitimate business purposes. Note that anonymised data cannot be deleted as we cannot trace it back to a specific entity.

7.4 Right to Restrict Processing

You may request that we limit how we use your information in specific circumstances, for example if you contest its accuracy.

7.5 Right to Data Portability

Where applicable, you can request a copy of your data in a structured, machine-readable format and transfer it to another organisation.

7.6 Right to Object

You can object at any time to our use of your information where we rely on legitimate interests as our lawful basis. We will stop processing your data for that purpose unless we can demonstrate compelling legitimate grounds which override your interests, rights and freedoms, or if the processing is for the establishment, exercise, or defence of legal claims.

Where we use your data for direct marketing, you have an absolute right to object and we will stop using your data for this purpose when you ask us to.

7.7 Rights related to Automated Decision Making and Profiling

If automatic decisions significantly affect you, you have the right to human intervention, express your concerns, or challenge the decision.

7.8 Withdrawing your Consent

If we process your data based on your consent (expressed or implied), you can withdraw it at any time by [contacting us](#). Withdrawal does not affect the lawfulness of processing before it was withdrawn and does not impact processing based on other lawful grounds.

7.9 Opting Out of Marketing and Promotional Communications

You can unsubscribe at any time by clicking the unsubscribe link in emails or by [contacting us](#). We may still need to send service-related communications.

7.10 Account Information

You can review, update, or delete your account information by [contacting us](#) or by visiting [your account page on the YCC Portal](#). Deletion requests will lead to the deletion of all your personal information from our active databases, with some data retained for fraud prevention, legal compliance, and troubleshooting purposes.

7.11 How to Exercise Your Rights

To exercise any of your privacy rights, you can [contact us](#) or visit [your account page on the YCC Portal](#). We may need to verify your identity before processing certain requests to protect your privacy.

We aim to respond within one month to all requests, extending the period if required for complex matters per applicable legislation.

7.11.1 Filing a Complaint

If you believe we have not handled your information in accordance with this Privacy Policy or applicable Data Protection Laws, you have the right to lodge a complaint.

In the first instance, please [contact us](#) to give us the opportunity to resolve your concern directly. If you remain unsatisfied, you can complain to the appropriate regulatory authority.

For United Kingdom residents, you should complain to the Information Commissioner's Office (ICO).

- Website: <https://ico.org.uk/make-a-complaint>
- Email: icocasework@ico.org.uk
- Phone: 0303 123 1113

For European Economic Area residents, you should complain to your local data protection authority.

- Website: https://www.edpb.europa.eu/about-edpb/about-edpb/members_en

You have the right to lodge a complaint with a supervisory authority without prejudice to any other administrative or judicial remedy.

8. Do Not Track Browser Controls

Most web browsers and some mobile operating systems include a Do Not Track ("DNT") feature or setting that you can activate to signal your preference not to have your online browsing activities tracked.

Currently, there is no uniform technology standard that requires websites and online services to respond to DNT signals, and we do not respond to DNT signals or other automatic mechanisms communicating your choice not to be tracked online.

If a recognised standard or legal requirement for responding to DNT signals is established in the future, we will update this Privacy Policy accordingly and inform you of any changes.

9. Do we make updates to this policy?

We may update this Privacy Policy from time to time to reflect changes in our data usage, or to stay compliant with relevant laws.

The “Last Updated” date at the top of this policy reflects the most recent version. Any changes will be posted on this page, and your continued use of the Website after updates are published means you accept the revised Privacy Policy.

If we make material changes, we will endeavour to notify you of such changes. However, we do also encourage you to review this Privacy Policy frequently to be informed of how we are protecting your information.

10. How can you contact us?

For privacy-based questions or to exercise your data protection rights in relation to this Privacy Policy, please contact the Director of Technology (our Data Protection Lead) using the methods outlined below.

Email: team@yorkcommunityconsulting.co.uk

Contact Form: <https://www.yorkcommunityconsulting.co.uk/contact>

Post: York Community Consulting, Careers and Placements, University of York, York, YO10 5DD, United Kingdom.