



Celora Holdings Careers Portal Privacy Policy

Effective Date: 14th September 2026

Last Updated: 14th September 2026

Celora Holdings ("Celora Holdings", "we", "us" or "our") is committed to protecting the privacy and personal data of individuals who use the **Celora Holdings Careers Portal** ("Careers Portal", "Portal" or "Service").

This Privacy Policy explains how Celora Holdings collects, receives, uses, stores, protects, retains and otherwise processes personal data in connection with the Careers Portal and associated recruitment services.

This Privacy Policy applies to candidates, applicants, prospective employees, current and former employees, individuals who create or use an account, and other individuals whose personal data is processed in connection with the Careers Portal.

By using the Careers Portal, you acknowledge that your personal data may be processed in accordance with this Privacy Policy and applicable data protection legislation.

Data Protection Legislation

Celora Holdings processes personal data in accordance with applicable data protection legislation, including, where applicable:

- the **United Kingdom General Data Protection Regulation ("UK GDPR")**;
- the **Data Protection Act 2018**;
- the **Privacy and Electronic Communications Regulations 2003 ("PECR")**; and
- other applicable UK legislation, regulations and regulatory requirements concerning privacy and data protection.

Where applicable, references to the UK GDPR include amendments, replacements or successor legislation in force from time to time.

Data Controller

For the purposes of the UK GDPR, the Data Protection Act 2018 and applicable data protection legislation, **Celora Holdings is the sole Data Controller** responsible for

determining the purposes and means of processing personal data collected, received, stored, used or otherwise processed through the **Celora Holdings Careers Portal**.

Celora Holdings determines why and how personal data is processed through the Careers Portal, including personal data relating to:

- candidate accounts;
- job applications;
- recruitment and selection;
- interviews and assessments;
- candidate communications;
- recruitment eligibility;
- identity and account verification;
- Discord and Roblox account linking;
- employment and former employment records;
- recruitment restrictions;
- Staff Blacklist records;
- onboarding;
- account security;
- fraud and abuse prevention; and
- administration and operation of the Careers Portal.

Celora Holdings is registered as a Data Controller with the Information Commissioner's Office ("ICO").

ICO Registration Reference: ZC175994

Registered Address:

Celora Holdings
Unit 168670
PO Box 7169
Poole
Dorset
BH15 9EL

Data Protection Officer:
dpo@celoraholdings.co.uk

Celora Holdings and the Careers Portal

The **Celora Holdings Careers Portal operates as a platform and service within the Celora Holdings corporate structure.**

The Careers Portal provides a centralised recruitment service through which vacancies across Celora Holdings and its associated companies, subsidiaries, departments and business operations may be advertised and administered.

Where an individual applies for a vacancy relating to a particular Celora Holdings company, subsidiary or business operation, the recruitment activity may be undertaken by authorised personnel associated with that organisation. However, **Celora Holdings remains the Data Controller for personal data processed through the Careers Portal**, unless a separate privacy notice expressly states otherwise.

Access by an authorised recruitment employee, HR representative, IT administrator, onboarding employee, subsidiary or business unit does not, by itself, make that person or organisation a separate Data Controller.

Data Protection Officer

Celora Holdings has designated a Data Protection Officer ("DPO") to act as a point of contact for data protection and privacy matters.

The DPO can be contacted at: dpo@celoraholdings.co.uk

For general matters, you may also contact:

General Enquiries: contact@celoraholdings.co.uk

Recruitment: recruitment@celoraholdings.co.uk

IT Services: itservices@celoraholdings.co.uk

Information We Collect

Depending on how you use the Careers Portal, Celora Holdings may collect and process the following categories of personal data.

Account Information

This may include:

- full name;
- username;
- email address;
- account credentials and authentication information;
- account creation and modification information;
- account status;
- account activity;
- account security information; and
- other information necessary to operate your Careers Portal account.

Recruitment Information

Where you submit an application, we may process:

- CVs and résumés;
- cover letters;
- application forms;
- employment history;
- previous employers;
- job titles and responsibilities;
- qualifications;
- certifications;
- skills and experience;
- professional information;
- references;
- interview information;
- assessment information;
- recruitment correspondence;
- application status;
- recruitment decisions;
- candidate feedback;
- onboarding information; and
- other information voluntarily provided during recruitment.

Application Information

We may retain information relating to applications, including:

- the vacancy applied for;
- date and time of application;
- application status;
- recruitment stage;
- communications regarding the application;
- interview invitations;
- interview attendance;
- interview outcomes;
- reasons for rejection where recorded;
- withdrawal of an application;
- acceptance of an offer;
- acceptance for an alternative role; and
- other recruitment administration records.

Verification Information

Celora Holdings may undertake appropriate verification activities to confirm information supplied during recruitment.

This may include verifying:

- identity;
- employment history;
- qualifications;

- experience;
- references;
- eligibility;
- required Discord server membership;
- required Roblox group membership; and
- information relevant to recruitment eligibility.

Where references are requested, information may be obtained from current or former employers or other referees where appropriate and lawful.

Candidates must provide accurate and truthful information. Information provided during recruitment may be checked where Celora Holdings considers verification necessary and proportionate.

Discord OAuth

The Careers Portal may provide functionality allowing candidates to securely link their Discord account using **Discord OAuth**.

OAuth is used to allow the Careers Portal to obtain authorised information from Discord without requiring the candidate to provide their Discord password to Celora Holdings.

Depending on the permissions and scopes authorised, Celora Holdings may receive information such as:

- Discord user ID;
- Discord username;
- display name;
- avatar or profile information;
- account identifiers;
- information relating to authorised server membership; and
- other information made available through the relevant OAuth permissions.

The exact information received will depend on the OAuth scopes requested and authorised.

Celora Holdings does **not intentionally request or store Discord passwords through the OAuth process**.

Discord is an independent third-party service. Discord's own processing of personal data is governed by its own privacy policy, terms and applicable legal obligations.

Roblox OAuth

The Careers Portal may provide functionality allowing candidates to securely link their Roblox account using **Roblox OAuth**.

OAuth allows candidates to authorise access to specified Roblox account information without providing their Roblox password to Celora Holdings.

Depending on the permissions and scopes authorised, Celora Holdings may receive information such as:

- Roblox user ID;
- Roblox username;
- display or account information;
- information relevant to Roblox Group membership;
- account identifiers; and
- other information made available through authorised OAuth permissions.

The exact information received will depend upon the OAuth scopes requested and authorised.

Celora Holdings does **not intentionally request or store Roblox passwords through the OAuth process.**

Roblox is an independent third-party service. Roblox's own processing of personal data is governed by its own privacy policy, terms and applicable legal obligations.

Purpose of Discord and Roblox Linking

Discord and Roblox account linking may be required or used to:

- verify candidate identity or account ownership;
- confirm eligibility for a vacancy;
- confirm required Discord server membership;
- confirm required Roblox Group membership;
- prevent fraudulent or duplicate accounts;
- maintain the integrity of the recruitment process;
- administer recruitment requirements;
- improve account security;
- investigate suspected misuse or abuse; and
- provide functionality associated with the Careers Portal.

Where account linking is mandatory for a particular vacancy or recruitment process, failure to provide the required information may prevent the candidate from progressing with that application.

OAuth Tokens and Authorisation Information

Where OAuth integrations are used, Celora Holdings may process technical authorisation information or tokens necessary to maintain the authorised connection.

OAuth information will be handled using appropriate security measures and will not be used for purposes unrelated to the authorised service unless otherwise permitted by law.

Where an OAuth connection is disconnected, expires or is no longer required, Celora Holdings will take appropriate steps to cease processing the associated authorisation information and delete it where retention is no longer necessary.

Former Employee Information

Where an applicant has previously been employed by Celora Holdings or an associated organisation, Celora Holdings may process relevant historical employment information where necessary for recruitment, employment administration, compliance, security or organisational purposes.

This may include:

- previous employment dates;
- previous role;
- employment status;
- relevant disciplinary records;
- resignation information;
- dismissal information;
- relevant recruitment restrictions;
- Staff Blacklist information; and
- other records legitimately retained from previous employment.

Such information will only be retained and used where there is a lawful and legitimate reason to do so.

Recruitment Restrictions and Staff Blacklist

Celora Holdings may maintain records relating to recruitment restrictions where necessary to protect the integrity, security and proper administration of recruitment.

This may include restrictions arising from:

- previous employment;
- resignation;
- dismissal;
- serious misconduct;
- previous recruitment decisions;
- abuse of the Careers Portal;
- fraudulent activity;
- repeated misuse of recruitment systems; or
- other legitimate organisational or security concerns.

Where an individual is subject to a Staff Blacklist or recruitment restriction, Celora Holdings may retain information necessary to administer that restriction.

Restrictions will be subject to appropriate review and will not be retained indefinitely where there is no continuing lawful basis or legitimate necessity for doing so.

Purposes of Processing

Celora Holdings may process personal data for the following purposes:

- creating and administering Careers Portal accounts;
- processing job applications;
- assessing candidates;
- arranging interviews;
- communicating with candidates;
- verifying candidate information;
- checking recruitment eligibility;
- confirming Discord and Roblox requirements;
- managing recruitment restrictions;
- administering Staff Blacklist records;
- managing successful candidates;
- facilitating onboarding;
- maintaining employment-related records;
- preventing duplicate or fraudulent accounts;
- maintaining platform security;
- detecting and investigating misuse;
- complying with legal obligations;
- establishing, exercising or defending legal claims;
- maintaining business records;
- improving the Careers Portal;
- maintaining technical infrastructure;
- responding to enquiries; and
- protecting Celora Holdings, its employees, candidates and users.

Lawful Bases for Processing

Celora Holdings will only process personal data where a lawful basis exists under applicable data protection legislation.

Depending on the circumstances, this may include:

Legitimate Interests

Celora Holdings may process personal data where necessary for its legitimate interests, provided those interests are not overridden by the individual's rights and freedoms.

Examples may include:

- recruitment administration;
- platform security;
- fraud prevention;
- recruitment eligibility;
- preventing duplicate accounts;
- maintaining recruitment records;

- protecting organisational systems; and
- managing recruitment restrictions.

Contractual Necessity

Personal data may be processed where necessary to take steps at an individual's request before entering into an employment relationship or to perform an agreement.

Legal Obligation

Personal data may be processed where necessary to comply with a legal or regulatory obligation.

Consent

Where consent is required, Celora Holdings may rely on consent as the lawful basis for processing.

Where processing is based solely on consent, individuals may withdraw their consent at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

Legal Claims

Personal data may be processed where necessary for the establishment, exercise or defence of legal claims.

Special Category Data

Celora Holdings may process special category personal data only where it is necessary and where an appropriate condition under applicable data protection legislation applies.

Where special category information is requested as part of recruitment or employment processes, Celora Holdings will seek to ensure that the information is handled appropriately and only used for legitimate purposes.

Candidates should not voluntarily provide unnecessary sensitive information through application forms, messages or other areas of the Careers Portal.

Recruitment Decision-Making

Applications may be assessed by authorised members of the Celora Holdings Recruitment Team and other authorised personnel involved in recruitment.

Candidate assessments may consider:

- suitability for the position;

- experience;
- qualifications;
- knowledge;
- skills;
- professionalism;
- application quality;
- interview performance;
- eligibility;
- previous relevant employment information; and
- other information relevant to the vacancy.

Celora Holdings may request additional information or conduct interviews where necessary.

Where automated decision-making or profiling producing legal or similarly significant effects is used, Celora Holdings will provide the information and safeguards required by applicable data protection legislation.

Recruitment Communications

Celora Holdings may contact candidates using the contact details provided through the Careers Portal.

Communications may include:

- application confirmations;
- application status updates;
- interview invitations;
- interview reminders;
- recruitment decisions;
- requests for additional information;
- onboarding information;
- account notifications;
- security notifications; and
- other recruitment-related communications.

Important recruitment communications may be sent to the registered email address associated with the candidate's account.

Sharing Personal Data

Celora Holdings may disclose personal data where necessary and lawful to:

- authorised recruitment personnel;
- authorised HR personnel;
- authorised IT Administrative Services personnel;
- authorised onboarding personnel;
- relevant personnel within Celora Holdings;

- Data Processors;
- hosting and infrastructure providers;
- email and communications providers;
- authentication and security providers;
- technical service providers;
- professional advisers;
- legal advisers;
- regulators and public authorities;
- law enforcement where legally required or permitted; and
- other parties where disclosure is necessary for a lawful purpose.

Celora Holdings will not sell personal data to third parties.

Data Processors

Celora Holdings may appoint third-party Data Processors to provide services necessary for operating the Careers Portal.

Processors may provide services including:

- website hosting;
- database hosting;
- cloud infrastructure;
- email delivery;
- authentication;
- security;
- monitoring;
- technical support;
- analytics;
- data storage; and
- other technology services.

Where required by law, Celora Holdings will have appropriate contractual arrangements with its Data Processors and will take reasonable steps to ensure that they provide appropriate security and data protection safeguards.

The use of a Data Processor does not transfer responsibility for the processing away from Celora Holdings. **Celora Holdings remains the Data Controller.**

International Transfers

Some service providers used by Celora Holdings may process personal data outside the United Kingdom.

Where personal data is transferred internationally, Celora Holdings will ensure that the transfer is carried out in accordance with applicable UK data protection legislation and that an appropriate transfer mechanism or safeguard is used where required.

This may include:

- UK adequacy regulations;
- appropriate safeguards;
- the UK International Data Transfer Agreement;
- the UK Addendum to EU standard contractual clauses; or
- another lawful transfer mechanism.

Data Security

Celora Holdings takes appropriate technical and organisational measures to protect personal data against:

- unauthorised access;
- unauthorised disclosure;
- accidental loss;
- destruction;
- alteration;
- misuse; and
- other unlawful processing.

Security measures may include access controls, authentication, encryption where appropriate, logging, monitoring, restricted administrative access and other security controls.

No online system can be guaranteed to be completely secure. However, Celora Holdings will take reasonable and appropriate measures to protect personal data under its control.

Recruitment Team Access

Access to candidate information is restricted to authorised personnel who require access for legitimate recruitment, HR, administrative or related purposes.

The **Celora Holdings Recruitment Team** may access information necessary to:

- review applications;
- communicate with candidates;
- conduct interviews;
- assess candidates;
- manage recruitment decisions;
- verify information; and
- administer recruitment processes.

IT Services Access

The **Celora Holdings IT Services Team** may access personal data where necessary for:

- account administration;
- technical support;
- security;
- system administration;
- OAuth integrations;
- investigation of technical incidents;
- fraud prevention;
- platform maintenance; and
- other legitimate IT or security purposes.

IT access is subject to appropriate access controls and should only be exercised where necessary.

Onboarding Team

Where an application is successful, information may be provided to authorised onboarding personnel for the purpose of facilitating onboarding and commencement of employment.

The onboarding email address is: onboarding@celoraholdings.co.uk

The onboarding mailbox is not actively monitored for general enquiries.

Candidates should direct recruitment-related questions to:
recruitment@celoraholdings.co.uk

Technical or account-related matters should be directed to:
itservices@celoraholdings.co.uk

Data Retention

Celora Holdings will retain personal data only for as long as it is reasonably necessary for the purposes for which it was collected or otherwise processed, unless a longer retention period is required or permitted by law.

There is no universal statutory retention period applicable to all recruitment information. Retention periods will depend on factors including:

- the nature of the information;
- the purpose for which it is retained;
- whether the individual was successful;
- whether the individual remains employed;
- legal and regulatory requirements;
- potential legal claims;
- security and fraud prevention requirements;
- recruitment restrictions; and
- the need to demonstrate compliance.

Celora Holdings will periodically review retained personal data and, where information is no longer required and there is no lawful reason for continued retention, it will be securely deleted, destroyed or anonymised as appropriate.

Unsuccessful Applications

Personal data relating to unsuccessful applications may generally be retained for a limited period following the final recruitment decision.

As an internal retention guideline, unsuccessful application records may generally be retained for **up to 12 months following** the final recruitment decision, subject to the circumstances of the individual record.

Where there is a legitimate reason to retain particular information for longer, such as legal claims, regulatory requirements, fraud prevention, recruitment restrictions or other lawful purposes, relevant information may be retained for the necessary period.

Withdrawn Applications

Where a candidate withdraws an application, Celora Holdings may retain relevant records for a limited period for administrative, security, legal and compliance purposes.

Withdrawn application information may generally be retained for **up to 12 months**, subject to applicable legal requirements and legitimate retention needs.

Interview Records

Interview-related information may be retained where necessary to administer recruitment, document recruitment decisions, respond to disputes or demonstrate compliance.

Interview records will not be retained indefinitely and will be reviewed in accordance with applicable retention requirements.

Successful Applications

Where an application results in employment, relevant recruitment information may become part of the individual's employment record.

Not all recruitment information will automatically become a permanent employment record.

Information that is no longer necessary will be deleted or securely disposed of in accordance with applicable retention requirements.

Recruitment Restriction Records

Information relating to recruitment restrictions or Staff Blacklist decisions may be retained for the duration of the relevant restriction.

Following expiry of a restriction, Celora Holdings will review whether continued retention remains necessary.

Information may be retained for longer where necessary to:

- establish or defend legal claims;
- prevent fraud;
- investigate serious misconduct;
- demonstrate compliance;
- protect the security of the Careers Portal; or
- satisfy another lawful requirement.

Discord and Roblox Data Retention

Discord and Roblox information obtained through authorised OAuth integrations will not be retained indefinitely.

Celora Holdings will retain such information only where it remains necessary for purposes including:

- account management;
- recruitment eligibility;
- verification;
- security;
- fraud prevention;
- recruitment records; or
- legal and compliance requirements.

OAuth credentials or tokens that are no longer required will be deleted or invalidated where appropriate.

Legal Holds

Where Celora Holdings reasonably anticipates or becomes involved in legal proceedings, regulatory investigations, disputes or potential legal claims, relevant information may be placed under a legal hold.

Information subject to a legal hold may be retained for as long as reasonably necessary for the relevant legal or regulatory matter, even where the ordinary retention period would otherwise have expired.

Account Deletion

Candidates may request deletion of their Careers Portal account and associated personal data.

Account deletion does not necessarily require immediate deletion of every record associated with the individual.

Celora Holdings may retain information where necessary to:

- comply with a legal obligation;
- establish, exercise or defend legal claims;
- prevent fraud or abuse;
- maintain security records;
- comply with regulatory requirements;
- administer recruitment restrictions; or
- satisfy another lawful requirement.

Where retention is required, the relevant information will only be retained for as long as necessary.

Data Subject Rights

Subject to applicable legal conditions and exemptions, individuals have rights concerning their personal data.

These may include:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restriction of processing;
- the right to data portability;
- the right to object to certain processing;
- rights relating to automated decision-making and profiling; and
- the right to withdraw consent where processing relies on consent.

These rights are not absolute and may be subject to legal exemptions and limitations.

Right of Access

You may request a copy of personal data that Celora Holdings holds about you.

This is commonly referred to as a **Subject Access Request ("SAR")**.

Requests should be sent to: dpo@celoraholdings.co.uk

Celora Holdings may take reasonable steps to verify your identity before releasing personal information.

Right to Rectification

You may request correction of inaccurate or incomplete personal data.

Where appropriate, Celora Holdings will correct or update the relevant information.

Candidates are responsible for ensuring that information submitted during recruitment remains accurate and up to date.

Right to Erasure

In certain circumstances, you may request that Celora Holdings erase personal data.

The right to erasure is not absolute. Celora Holdings may lawfully retain information where there is a continuing legal basis or where an applicable exemption applies.

Right to Restriction

You may have the right to request restriction of processing in circumstances provided by applicable data protection legislation.

Where processing is restricted, Celora Holdings may continue to store the information but will generally not otherwise process it except where legally permitted.

Right to Object

You may have the right to object to processing based on legitimate interests or to certain forms of direct marketing.

Where an objection is received, Celora Holdings will assess whether it is required to stop the relevant processing or whether a lawful exception applies.

Data Portability

Where applicable, you may have the right to receive personal data provided to Celora Holdings in a structured, commonly used and machine-readable format and request its transmission to another controller.

This right only applies in circumstances established by applicable law.

Withdrawal of Consent

Where Celora Holdings relies on consent, you may withdraw that consent at any time.

Withdrawal of consent will not affect processing carried out before consent was withdrawn.

Exercising Your Rights

Privacy and data protection requests should be submitted to:

Data Protection Officer dpo@celoraholdings.co.uk

You may also contact:

General Enquiries: contact@celoraholdings.co.uk

Recruitment: recruitment@celoraholdings.co.uk

IT Services: itservices@celoraholdings.co.uk

Celora Holdings will generally respond to valid data protection requests within the applicable statutory timeframe.

Identity Verification

To protect personal data from unauthorised disclosure, Celora Holdings may request reasonable information to verify the identity of an individual making a data protection request.

Where identification information is requested, it will be used for the purpose of verifying the request and protecting personal data.

Complaints

If you have concerns regarding how Celora Holdings processes your personal data, you should initially contact the Data Protection Officer: dpo@celoraholdings.co.uk

You also have the right to lodge a complaint with the **Information Commissioner's Office ("ICO")** where you believe that your personal data has been processed unlawfully or that your data protection rights have been infringed.

Cookies and Similar Technologies

The Careers Portal may use cookies and similar technologies necessary to operate, secure and maintain the Service.

These may be used for purposes including:

- account authentication;
- session management;
- security;
- remembering preferences;
- maintaining functionality;

- preventing abuse; and
- understanding technical usage where applicable.

Where consent is legally required for a particular cookie or technology, Celora Holdings will obtain consent before using it.

Technical and Security Information

When you access the Careers Portal, technical information may be automatically generated or collected.

Depending on the system configuration, this may include:

- IP address;
- browser type;
- device information;
- operating system;
- login times;
- authentication events;
- security logs;
- error information;
- pages or functions accessed;
- account activity; and
- other technical information required to operate and secure the Service.

This information may be processed for security, troubleshooting, fraud prevention, system administration and legal compliance.

Fraud and Abuse Prevention

Celora Holdings may process personal data to detect, prevent and investigate:

- fraudulent applications;
- duplicate accounts;
- false information;
- impersonation;
- unauthorised account access;
- abuse of recruitment processes;
- attempts to circumvent recruitment restrictions;
- misuse of OAuth integrations;
- security incidents; and
- other misuse of the Careers Portal.

Where necessary, relevant information may be retained for as long as reasonably required to protect the Careers Portal and Celora Holdings.

Accuracy of Information

Celora Holdings seeks to ensure that personal data is accurate and appropriate for the purposes for which it is processed.

Candidates should notify Celora Holdings where information held about them is inaccurate or has changed.

Data Minimisation

Celora Holdings will seek to collect and process only personal data that is adequate, relevant and necessary for the purposes for which it is processed.

Individuals should not submit unnecessary personal or sensitive information through the Careers Portal.

Confidentiality

Personal data will only be accessible to individuals who have a legitimate business or operational requirement to access it and who are appropriately authorised.

Personnel with access to confidential candidate information are expected to maintain the confidentiality and security of that information.

Personal Data Breaches

Celora Holdings maintains procedures for identifying, investigating and responding to personal data breaches.

Where a personal data breach occurs, Celora Holdings will assess the incident and take appropriate action in accordance with applicable data protection legislation.

Where notification to the ICO or affected individuals is legally required, Celora Holdings will make the relevant notification within the applicable statutory timeframe.

Third-Party Services

The Careers Portal may integrate with third-party services, including Discord, Roblox and other technology providers.

These services may process personal data independently of Celora Holdings.

Celora Holdings does not control the privacy practices of independent third-party services. Individuals should review the privacy policies and terms applicable to those services.

Where Celora Holdings uses a third party as a Data Processor, the processing will be governed by the appropriate contractual and data protection arrangements.

Children and Young Persons

The Careers Portal is intended for individuals who satisfy the applicable minimum age and eligibility requirements for the relevant employment or recruitment process.

Where personal data relating to a young person is processed, Celora Holdings will take appropriate account of applicable legal requirements and the circumstances of the processing.

Changes to This Privacy Policy

Celora Holdings may update this Privacy Policy from time to time to reflect:

- changes to the Careers Portal;
- changes to recruitment processes;
- changes to technology;
- changes to third-party integrations;
- changes to applicable law;
- regulatory guidance; or
- changes to how personal data is processed.

The latest version will be made available through the Careers Portal.

Where appropriate, material changes may be communicated to users through the Careers Portal or registered contact information.

Governing Framework

This Privacy Policy is governed by applicable law in the United Kingdom and should be read alongside applicable Celora Holdings policies, terms and procedures.

Nothing within this Privacy Policy removes or limits any statutory rights that an individual has under applicable data protection legislation.

Contact Information

For privacy and data protection matters:

Celora Holdings

Unit 168670
PO Box 7169
Poole
Dorset
BH15 9EL

Data Protection Officer: dpo@celoraholdings.co.uk

General Enquiries: contact@celoraholdings.co.uk

Recruitment: recruitment@celoraholdings.co.uk

IT Services: itservices@celoraholdings.co.uk

Website: www.celoraholdings.co.uk

Careers Portal: www.careers.celoraholdings.co.uk

ICO Registration Reference: ZC175994

Privacy Policy Acknowledgement

By creating an account, submitting an application or otherwise using the Celora Holdings Careers Portal, you acknowledge that you have been provided with access to this Privacy Policy.

This acknowledgement does not remove or restrict any rights you have under applicable data protection legislation.