CORNDEL

Data Protection Policy

Document Approval

Document Owner	Approver	Version Approved	Date	Public Facing Y/N
Annemarie Schofield	Mushall Khan	1.0	20/01/2018	Y
Richard Bridge and Jimi Gill	Elizabeth Underwood	2.0	22/10/2018	Y
Richard Bridge and Jimi Gill	Elizabeth Underwood	3.0	17/04/2019	Y
Richard Bridge and Jimi Gill	Elizabeth Underwood	4.0	26/10/2020	Y
Richard Bridge (Data Protection Officer	Laura Bowey	5.0	18/01/2024	Y
Richard Bridge (Data Protection Officer)	Alan Gilles (Director of IT)	6.0	22/05/2025	Y
Richard Bridge (Data Protection Officer)	Alan Gilles (Director of IT)	7.0	15/08/2025	Y

Document Revision History

Issue	Date Issued	Date Effective	Purpose of Issue and Description of Amendments
1.0	20/1/2018	15/01/2018	Original
2.0	22/10/2018	22/10/2018	Revision
3.0	17/04/2019	17/04/2019	Revision
4.0	26/10/2020	26/10/2020	Revision
5.0	18/01/2024	18/01/2024	Revision and update to include AI use
6.0	22/05/2025	22/05/2025	Update to include Data Retention and Deletion and make ISO 27001 compliant
7.0	15/08/2025	15/08/2025	Update following review by lawyer

1.0 Policy Statement

1.1 Corndel aims to create and nurture a transparent and supportive employee culture centred around a data protection compliance framework where employees are informed, self-aware and thoughtful in how they handle personal data at all times.

1.2 Everyone has rights with regard to the way in which their personal data is handled. Corndel Group (See **Definitions** section below - referred to as 'Corndel' in this document) is an apprenticeship, degree, and commercial training provider, specialising in adult technical and vocational education. During our activities, we collect, store and process personal data, including some limited sensitive data (also referred to as "**special category data**", see **Definitions** section below), about our employees, customers (employers/learners/students/line managers), suppliers and other third parties. We recognise that the correct and lawful treatment of this data has an important role to play in maintaining Corndel's reputation and conducting business operations successfully.

1.3 Corndel collects, evaluates and stores (collectively referred to as "**processing**", see **Definitions** section below) a range of personal and sensitive data and records of learning. We process this data to facilitate the learning of people on our programmes, provide appropriate reporting to employers on the progress of their employees, and to manage and support Corndel employees, as well as to comply with the rules of our regulators, and other legal and regulatory requirements.

1.4 Some limited personal data such as names and emails are provided to us directly by employers (our clients), but other personal and sensitive data is provided to Corndel by the learners themselves directly into a secure online learning and management portal.

2.0 About this Policy

2.1 This policy (and other documents referred to in it) sets out the basis on which we will process any personal data we collect from data subjects (see **Definitions** section below), or that is provided to us by data subjects or other sources. Our data subjects include current, past and prospective learners, client/employer contacts and others that we communicate with, as well as employee details. We act as data controller (see **Definitions** section below) with regards to the personal data we collect of these data subjects.

2.2 This policy applies to all personal data we process regardless of media, method of storage etc. All personal data are subject to certain legal safeguards specified in the Data Protection Act 2018 (the "**Act**"), the UK General Data Protection Regulations ("**UK GDPR**") and other regulations. Corndel does not use paper-based records.

2.3 This policy applies to all Corndel employees (**data users**), who must read, understand and comply with this policy when processing personal data on Corndel's behalf. Data protection is the responsibility of everyone with Corndel and sets out what we expect from our employees when handling personal data to enable Corndel to comply with applicable law. Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

2.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy has been approved by Corndel's senior management and sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data. This policy (together with other documents referred to within it) is an internal document and cannot be shared with third parties without prior authorisation from our DPO.

3.0 Definitions

3.1 **Corndel Group** ("**we**", "**our**", "**us**", "**Corndel**") comprises Corndel Limited of 5th Floor, 80 Old Street, London, EC1V 9AZ, company number 10369857 and Corndel Education Limited (trading as Corndel College London or CCL) of 5th Floor, 80 Old Street, London, EC1V 9AZ, company number 13486506, and their associated brands.

Corndel Group is wholly owned by CoEdu Group Limited (trading as Galileo Global Education) which in turn is owned by Galileo Global Education UK Holding Limited.

Whichever of Corndel Ltd or Corndel Education Ltd first collect the data, will be the controller of that personal data. In addition, when processing of personal data is undertaken by other companies of the Corndel Group (i.e. Corndel Ltd or Corndel Education Ltd) for their own independent purposes, these companies will also be controllers of that personal data.

3.2 **Data** is information which is stored electronically, on a computer, or in any other medium, including personal data.

3.3 **Data subjects** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.4 **Data controllers** are the people, or organisations, who determine the purposes and the way, any personal data is processed. They are responsible for establishing practices and policies in line with the Act and UK GDPR.

3.5 **Data processors** include any person or organisation that processes personal data on our behalf in accordance with our instructions. Data processors must protect the personal data they handle in accordance with this policy, mandatory processor contractual obligations, and any applicable data security procedures/legislation, at all times.

3.6 **Personal data** means data relating to a living individual who can be identified, or is identifiable from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.7 **Personal Data Breach** means any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

3.8 **Privacy by Design** means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR.

3.9 **Processing** is any activity that involves use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.10 **Sensitive personal data** (also referred to as "**special category data**" in accordance with its definition in the UK GDPR) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual identity and orientation. Sensitive personal data can only be processed under strict conditions, including an additional lawful basis for processing, i.e. a lawful basis for processing under Article 6 of the UK GDPR and a further lawful basis under Article 9 of the UK GDPR for processing special category data.

3.11 **SaaS** is Software as a Service. Corndel is entirely cloud based for all our IT and does not own or manage its own servers or network. It uses a variety of reputable SaaS which have been put through an appropriate due diligence process including checking their data security arrangements.

3.12 **ROPA** is the Register of Processing Activities. It outlines Corndel's data processing activities, including how personal data is collected, stored, used, and transferred. This document is a key element of demonstrating compliance with data protection laws and regulations.

4.0 Data Protection Principles

4.1 Anyone processing personal data must comply with the following principles relating to the processing of personal data set out in the UK GDPR which require personal data to be:

- Processed fairly, lawfully and in a transparent manner (**lawfulness, fairness and transparency**),
- Processed only for specified, explicit and legitimate purposes and in an appropriate way (**purpose limitation**),
- Adequate, relevant and not excessive for the purpose (**data minimisation**),
- Accurate and where necessary kept up to date (**accuracy**),
- Not kept longer than necessary for the purpose (**storage limitation**),
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unlawful or unauthorised processing and against accidental loss, destruction or damage (**security, integrity and confidentiality**),
- Made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (**data subject's rights and requests**),

Further, we are responsible for and must be able to demonstrate compliance with the above-mentioned principles (**accountability**).

5.0 Fair, Lawful and Transparent Processing

5.1 The Act/UK GDPR are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

5.2 For personal data to be processed lawfully, fairly and in a transparent manner, they must be processed on the basis of one of the legal grounds (often referred to as "**lawful basis**" or "**condition**") set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing personal data as data controllers in the course of our business, we will ensure that those requirements are met.

5.3 We must identify and document the lawful basis being relied on for each processing activity. The principle of accountability (as set out above) requires us to be able to demonstrate that we are complying with the Act/UK GDPR and have appropriate policies and processes. This means that we need to be able to show that we have properly considered which lawful basis applies to each processing purpose and can justify our decision.

5.4 Processing any sensitive data requires 2 lawful bases for processing, i.e. a lawful basis for processing personal data under Article 6 of the UK GDPR and a further lawful basis under Article 9 of the UK GDPR for processing sensitive data. We document in the Corndel ROPA both lawful bases for processing.

6.0 Notifying Data Subjects (Transparency)

6.1 If we collect personal data directly from data subjects, we will provide them with access to our Privacy Policies and Notices to ensure they are informed about:

- the purpose or purposes for which we intend to process that personal data,
- how we will process their data in accordance with UK GDPR,
- what types of data we will collect,
- the types of third parties, if any, with which we will share or to which we will disclose that personal data,
- If the data is to be transferred outside the EU/UK jurisdiction,
- The legal basis for the processing.

6.2 We will also inform data subjects whose personal data we process that Corndel is the data controller with regards to that data.

7.0 Processing for Limited Purposes

7.1 In the course of our business, we may collect and process the personal data set out in the Corndel ROPA and in the Data Processing Schedules in our Privacy Policies and Web Privacy Notices. This may include personal data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and personal data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2 We will only process personal data for the specific purposes set out in the Corndel ROPA and in the Data Processing Schedules in our Privacy Policies and Web Privacy Notices or for any other purposes specifically permitted by the Act/UK GDPR. We will set out those purposes to the data subject when we first collect the data or as soon as possible thereafter via our Privacy Notices.

7.3 Such personal data is processed and securely stored in the SaaSs we use, and is only accessible by Corndel's employees.

7.4 Any changes to the purposes of processing must first be discussed with the Corndel DPO for advice on how to do this in compliance with both the law and this policy.

8.0 Adequate, relevant and non-excessive processing (data minimisation)

8.1 We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

8.2 We may only process personal data when performing your job duties require it. We cannot process personal data for any reason unrelated to our job duties. We may only collect personal data that is required for our job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

8.3 We must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the details set out in our ROPA.

9.0 Accurate Data

9.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at appropriate intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. Storage Limitation

10.1 We will maintain retention policies and procedures to ensure personal data is deleted after an appropriate time unless a law requires that personal data to be kept for a minimum time.

10.2 We must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

10.3 We will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with our Data Retention Policy (see section 18 Data Retention and Deletion below) and the retention periods as set out in the Corndel ROPA. This includes requiring third parties to delete that personal data where applicable.

11 Data Security

11.1 We will process all personal data we hold in accordance with our Privacy Policies and Notices and take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

11.2 We must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles because we are responsible for, and must be able to demonstrate, compliance with the data protection principles. This means that we must have adequate resources and controls in place to ensure and to document the Act/UK GDPR compliance including:

- where required in accordance with the UK GDPR) appointing a suitably qualified DPO and an executive accountable for data privacy,
- implementing Privacy by Design when processing personal data and completing Data Protection Impact Assessments (**DPIAs**) where processing presents a high risk to rights and freedoms of data subjects,
- integrating data protection into internal documents including this Policy, related policies or Privacy Notices,
- regularly training Corndel personnel on the Act/UK GDPR, this Policy, related policies, and data protection matters including, for example, a data subject's rights, consent, legal basis, DPIA and personal data breaches. We must maintain a record of training attendance by Corndel personnel,
- and regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

11.3 Personal data will only be transferred to a data processor/SaaS if they can provide us with evidence that they have in place adequate security measures that Corndel has assured are appropriate and meet our standards. (See Corndel's Information Security Policy for more details on how we secure data).

11.4 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it. Corndel segregates access to data within the SaaSs we use on the basis of need to know/need to use using account permissions and group structures.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Corndel will ensure that the SaaSs we use have appropriate Recovery Time Objectives (RTO) to maintain Corndel's access to the data.

11.5 We must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Act/UK GDPR and relevant standards to protect personal data.

12 Training and Audit

12.1 We are required to ensure all Corndel personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

12.2 Employees must attend all mandatory data privacy-related training and ensure their steam undergo similar mandatory training.

12.3 We must regularly review all the systems and processes under our control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

13 Reporting a personal data breach

13.1 The UK GDPR requires data controllers to notify any personal data breach to the ICO and, in certain instances, the data subject.

13.2 We have put in place procedures to deal with any suspected personal data breach and will notify the data subject or any applicable regulator where we are legally required to do so.

13.3 If a personal data breach has occurred, do not attempt to Investigate the matter. Immediately report the incident to the Corndel GDPR Helpdesk mailto:gdpr@corndel.com. Preserve all evidence relating to the potential personal data breach.

14 Data Subjects' Rights and Requests

A data subject has rights when it comes to how we handle/process their personal data (**data subject's rights and requests**). These include rights to:

1. You have the right to request access to your personal data	Often referred to as a "**data subject access request**", you have the right to request confirmation that your personal data is being processed, access to your personal data (through us providing a copy) and other information about how we process your personal data. This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
2. You have the right to ask us to rectify your personal data	You have the right to request that we rectify your personal data if it is not accurate or not complete. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
3. You have the right to ask us to erase your personal data	In certain circumstances, you have the right to ask us to erase or delete your personal data where there is no reason for us to continue to process your personal data. This right would apply if we no longer needed to use your personal data to provide products and/or services to you, where you withdraw your consent for us to market to you, or where you object to the way we process your personal data (see right 6 below).
4. You have the right to ask us to restrict or block the processing of your personal data	You have the right to ask us to restrict or block the processing of your personal data that we hold about you. This right applies where you believe the personal data is not accurate, you would rather we block the processing of your personal data rather than erase your personal data, where we don't need to use your personal data for the purpose we collected it for but you may require it to establish, exercise or defend legal claims.
5. You have the right to port your personal data	You have the right to obtain and reuse your personal data from us to reuse for your own purposes across different services. This allows you to move personal data easily to another organisation, or to request us to do this for you.

6. You have the right to object to our processing of your personal data	You have the right to object to our processing of your personal data based on our legitimate interests, unless we can demonstrate that, on balance, our legitimate interests override your rights, or we need to continue processing your personal data for the establishment, exercise or defence of legal claims.
7. You have the right not to be subject to automated decisions	(Where applicable) you have the right to object to any automated decision making, including profiling, where the decision has a legal or significant impact on you.
8. You have the right to withdraw your consent	You have the right to withdraw your consent where we are relying on it to use your personal data.

A Data Subject may also report a complaint to our regulator, the Information Commissioner's Office (ICO) if they feel that Corndel has not addressed their concern in a satisfactory manner.

Contact details for the Information Commissioner's Office (ICO) can be found at https://ico.org.uk/global/contact-us/contact-us-public/

14.1 **Data subjects must make a formal request to exercise any of the above rights. This must be made in writing to either gdpr@corndel.com or to: The Data Protection Officer, Corndel Limited of 5th Floor, 80 Old Street, London, EC1V 9AZ.**

14.2 Corndel has 30 days to respond to any Data Rights requests.

14.3 Employees who receive a written request should forward it to the Corndel Data Protection Officer **immediately** at gdpr@corndel.com.

14.4 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

14.5 Our employees will refer a request to the Corndel Data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal data.

15 Processing of Data using AI

15.1 **Legal Framework:** Corndel understands that any use of AI where personal data is used to train, test or deploy Artificial Intelligence (AI) is governed by all relevant existing legislation such as the Data Protection Act (2018), UK GDPR and The Equality Act 2020 for example. Corndel is committed to ensuring that any use of AI complies with applicable data protection laws, and appropriate safeguards are implemented to protect the privacy and security of personal data.

Employees involved in the development, deployment, or maintenance of AI systems will receive appropriate training on data protection and privacy to ensure compliance with legal requirements and internal policies:

- Corndel Staff AI Policy
- Corndel AI Policy for Learners

Where appropriate the DPO may require a DPIA to be completed prior to roll out of any new AI tools. Please consult with our DPO regards any new projects involving AI where personal data is used to train, test or deploy it at the earlier opportunity.

16 Transferring Personal Data to a Country Outside the EEA

16.1 Corndel will not normally transfer personal data that we hold outside of the UK and/or the European Economic Area ("**EEA**"), In cases where we do have to, we will ensure that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms and has a current Adequacy Agreement with the UK;
- Appropriate safeguards are in place such as some ICO approved legal basis to govern the transfer such as the UK Extension to the EU/US Data Privacy Framework, which ensures

adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights as set out in the UK GDPR and the Act., EU standard contractual clauses (often referred to as the "**EU SCCs**") approved for use in the UK, an approved code of conduct or a certification mechanism.

- The data subject has given explicit consent to the proposed transfer after being informed of any potential risks.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims, or to protect the vital interests of the data subject.

16.2 Subject to the requirements in Clause 14.1 above, personal data we hold may also be processed by employee operating outside the EEA who works for us or for one of our suppliers. That employee may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

17 Disclosure and Sharing of Personal Information

17.1 We may share personal data we hold with any member of The Corndel Group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in section 1159 of the Companies Act 2006.

17.2 We may also disclose personal data we hold to third parties:

- If we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets; and
- If we, or substantially all our assets, are acquired by a third party, personal data we hold will be one of the transferred assets.
- If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

17.4 We may also share personal data we hold with selected third parties for the purposes set out in the Corndel ROPA.

17.5 You may only share the personal data we hold externally with third parties, such as our service providers, if:

- A valid lawful basis has been determined.
- They need to know the information for the purpose of providing the contracted services and we have determined the data protection capacity in which they will be processing the personal data, i.e. as data processor or data controller (or both).
- Sharing the personal data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained.
- The third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place.
- The transfer complies with any applicable cross-border transfer restrictions.
- and a fully executed data sharing or processing written contract that contains (where the third party is acting as our processor) UK GDPR-approved processor clauses or (where the third party is acting as our controller) our approved data sharing provisions are in place.

17.6 Any queries regarding a proposed arrangement to share personal data should first be checked with the Corndel DPO.

18 Data Retention and Deletion

18.1 Corndel manages data retention and secure disposal in alignment with business requirements and legal obligations. Various pieces of legislation and regulations outline retention requirements. These include, but not limited to:

- The UK General Data Protection Regulations (the UK GDPR)
- Data Protection Act 2018 (DPA 18)
- Finance Act 2016 (Apprenticeship Levy)
- Safeguarding Vulnerable Groups Act 2006 and Care Act 2014
- Ofsted regulations
- HMRC regulations

18.2. Retention Periods

18.2.1 Retention periods are determined by legislation and/or business need.

18.2.2 Details of retention periods are set out in the Corndel ROPA.

It is the responsibility of the relevant IAO to ensure that the details in the ROPA are correct including:

- Retention periods are not excessively long and are consistent with this policy.
- Retention triggers are clear and consistent.
- The correct retention source/reason has been identified.

18.2.3 The ROPA is a 'living' document and is reviewed regularly by the Corndel DPO with input from the IAOs.

18.2.4 We are under an obligation to keep and maintain our ROPA so that it provides an accurate and up-to-date reflection of our processing activities, Any new projects involving the collection / processing of different types of personal data, or changes to the way we currently collect and use personal data must be referred to the DPO who is responsible for the maintenance of our ROPA.

18.3 Weeding

18.3.1 Redundant, obsolete, or trivial (ROT) data should be periodically destroyed without requiring approval. Corndel conducts an annual company-wide weeding event usually in May following the All-Staff Annual IT and Data Security Update training.

18.3.2. Below are common examples of data which are usually of limited value once they are no longer in use and can be weeded through housekeeping. This should not be seen as an exhaustive list.

- **Drafts:** Delete obsolete draft documents once the final version is published.
- **Tracking Documents:** Remove personally generated tracking documents after use.
- **Duplicates:** Avoid retaining duplicate data to prevent confusion.
- **Emails**: Save important emails to shared spaces for evidence of decisions or actions. Delete most emails once the conversation has concluded
- **Limited Long-Term Value:** Weed out data with limited long-term operational value as soon as it is no longer required.

18.3.3. Where appropriate Corndel will use automated processes for the regular deletion of data in line with retention and deletion periods set out in the ROPA.

18.4 Destruction

Data not needed by the organization and lacking archival value should be securely destroyed in a manner appropriate to the confidentiality/risk level of the data. When data is destroyed, all copies of the data (both digital and physical) should be destroyed at the same time

18.5 Anonymisation of Data

18.5.1 Learner data held in the SQL database will be anonymized at the end of the retention period for ongoing analysis.

18.5.2 We will ensure that the following as a minimum is deleted from the data: name, email address, address, telephone numbers, DOB, ULN, job title, address data and line management data, review responses and other identifiable data.

18.6.3 We will retain the learner ID and Programme ID in the tables to link data sets together. These IDs are provided by Aptem and after anonymising data in our Database we will arrange for all data to be deleted from Aptem so removing the possibility of cross referencing the ID we retain in the SQL database to identify a learner.

18.6 Roles and Responsibilities

18.6.1 All Corndel staff are responsible for managing data in accordance with this Policy as set out earlier in this policy.

18.6.2 The following roles have responsibilities with regards Corndel data:

- **Corndel Data Protection Officer** (DPO) works with the departmental IAOs to advise, support, and ensure that this policy is being appropriately and consistently implemented.
- **Information Asset Owners (IAO)**: IAOs are Departmental SLT leads responsible for ensuring in their departments the legal collection of personal data they require, its secure holding and processing, the setting of retention periods and that disposal of data is conducted at the appropriate times and using appropriate methods. They are also responsible for ensuring their department cooperates in a timely way with the DPO with the completion and regular updating of the Corndel ROPA.
- **Information Asset Managers (IAM)**: IAMs assist the IAOs and are operationally responsible for actioning the requirements of the Corndel Data Protection Policy including the completion of the ROPA, keeping the DPO up to date with changes relevant to the ROPA and the good management of the personal data held in their departments including its timely deletion as set out in the ROPA.

19 Complaints

19.1 Should data subjects have any complaints (not data protection related); they are advised to refer to Corndel's Complaints Policy and follow the procedure accordingly.

19.2 Key point of contact regarding data protection enquiries and complaints is:

Corndel's Data Protection Officer who can be contacted at gdpr@corndel.com

19.3 A Data Subject may also lodge a complaint regarding how we have handled their data with our regulator the Information Commissioner's Office (ICO), which can be contacted at https://ico.org.uk/global/contact-us/contact-us-public/

20 Changes to this Policy

20.1 We keep this policy under review and reserve the right to change this policy at any time.

20.2 This policy does not override any applicable national data privacy laws and regulations in countries where we operate.