NEWTON

PRIVACY HUB - TECHNICAL AND ORGANISATIONAL MEASURES

TECHNICAL

- **Technical Facilities and Measures.** Our internal Information Security team implement and enforce extensive technical facilities and measures across the Newton network and on all Newton-owned devices. We use a minimum of AES128 encryption on all Newton devices, and the majority now use AES256. We ensure that:

    - All devices are protected by firewalls
    - Email and internet traffic is subject to security monitoring
    - All devices are routinely patched with security updates
    - The user lifecycle is managed and audited, including password security
    - Malware and antivirus solutions are deployed on every device

- **Regular Testing, Assessment and Evaluation of Effectiveness of Measures.** Our technical facilities and measures are independently audited on at least an annual basis as part of our recertification for ISO 27001 and Cyber Essentials Plus. This requires us to keep all relevant policies (including data protection and information security policies) under review at least annually and includes testing, assessing and evaluating the effectiveness of both the policy and the measures which underpin those policies.

  However, we believe that it is important to test, assess and evaluate the effectiveness of our measures more frequently than this. Therefore, our Information Security Group meets at least monthly to discuss our current measures and how they are operating.

ORGANISATIONAL

- **Information Security Group.** We have a cross-functional, internal Information Security Group which is responsible for implementing and monitoring Newton's Information Security processes (including UK GDPR-compliance). This includes representation from legal, IT, assurance, finance, HR and learning and development. It is chaired by Newton's COO.

- **Continuous Improvement.** A key tenet of Newton's methodology is continuous improvement. We also apply this principle to our Information Governance and UK GDPR policies, processes and controls which we keep under constant review to ensure that they are always up-to-date, reflect current best practice and are able to effectively anticipate new threats and legislative developments.

- **Background checks on employees.** We carry out enhanced DBS checks (as a minimum) on all Newton consultants before they are assigned to any programme working in our public cluster (which includes local government, central government and the NHS). Where required, we also ensure that all consultants working on a particular programme are BPSS or SC cleared.

- **Staff Training.** We provide extensive Information Governance and UK GDPR training to all our staff. All Newton consultants spend their first four weeks on an intensive induction scheme to ensure that they conform with all Newton methodology, processes and policies. This includes modules on Information Security, Cybersecurity and UK GDPR compliance, and ensures that all Newton staff understand that all

information should be treated with the highest levels of confidentiality and respect. It also ensures that all employees are made aware of our internal systems and processes. Newton's learning and development programme includes regular refresher training on information security and data protection. All employees working within our public cluster complete additional training, including specifically on any data sharing and processing arrangements agreed with the client for that programme and client specific information security policies.

- **Transfers of personal data outside the EU (if such transfers will take place).** We usually only transfer personal data outside of the UK to countries in respect of which a UK adequacy decision has been made (including the EU). If it were necessary to transfer personal data to a third party and this would involve transferring personal data to a country where no adequacy finding has been made, we would work with the client to ensure that the transfer is made not only in a way which is compliant with the UK GDPR (e.g. by using standard contractual clauses), but that the personal data is also protected in practice. For example, by asking the third party recipient of any such data to complete our information security questionnaire to provide assurance on the technical facilities and measures in place to protect the personal data in practice. All responses to these questionnaires are reviewed by our Information Security Group (comprising both legal and IT experts) and no transfers take place until approval has been given.

- **Records of Personal Data Processing Activities.** Our legal team record personal data processing activities and personal data categories into our Article 30 processing registers which are held and maintained by them. At the start of every project we work with our client to put in place a DPA. Part of this process involves identifying and recording (in the DPA) the personal data processing activities which will need to be carried out and the specific personal data we will need to access. Our Article 30 processing register is updated with this information. Our legal team also have regular touch points with programme managers to ensure that the register is kept up to date as the project continues and any new processing activities/categories are added.

- **How we deal with Data Incidents.** Newton's culture, training, policies and processes mitigate the risk of data incidents occurring. However, if a breach were to occur, we have robust internal processes to immediately address the situation.

  We operate a P2 (low), P1 (high), & P0 (business critical) incident management system with agreed escalation routes. Our processes include the following steps:

  i. Incidents are logged and prioritised according to severity and assigned an incident handler responsible for implementing any corrective actions

  ii. Understand and categorise the breach or contravention, including data type, format, method of transfer, parties involved or impacted, risks and implications

  iii. Promptly inform all relevant parties (for example, the client and, if required, the ICO)

  iv. Contain the incident by putting in place actions to mitigate the impact of the breach or contravention

v. Log the contravention or breach, its impact and the actions taken in response in a register managed by Newton's assurance team. The register is reviewed periodically, together with the latest best practice, to consider how we can improve our policies, processes and training

Whilst going through our incident management process as described above, we back up critical data, process personal data in line with legislation and ensure that regression back to the 'as is' state is possible at key transition points. We review, update (if required) and adhere to client business continuity and disaster recovery plans.

In the extremely rare case of a high impact breach or repeat contraventions, we trigger a full "root cause analysis" and implement corrective actions to mitigate future occurrences and improve our processes and technology, with owners, deadlines and budget. Where appropriate, we share our experience with industry to inform best practice.

HOW WE WORK WITH CLIENTS

Our teams have extensive experience working on programmes involving complex information security and personal data compliance requirements and have appropriate technical facilities and measures (including systems and processes) to ensure compliance with the data protection legislation and to ensure the protection of the rights of data subjects. Our technology and legal teams support Newton on how to safely handle confidential, personal (including special category) data. As well as dealing with sensitive information in the public sector we are also experienced in working in OFFICIAL-SENSITIVE and List-X data environments.

When working with sensitive data we engage early with clients to ensure data is at the forefront of project planning. We adhere to all of our client organisation certifications and requirements which could include working entirely on the client network and systems. Where any data needs to be transferred from the client's system to Newton's system, we can provide a Secure File Transfer Protocol which ensures that data is also secured in transit.

- **Set up.** Before starting any work, we agree a comprehensive approach to data, including putting in place a Data Processing Agreement (DPA), with our client where appropriate. During the shaping phase of any programme, we proactively engage with our clients, alongside the programme sponsor and Data Protection Officer as appropriate, to rapidly agree an approach to data sharing and processing. This includes agreeing the data required to successfully complete the programme, the timeline for such data to be provided and agreeing a comprehensive DPA. When working with our clients on transformation programmes, Newton will generally be the data processor and the client will remain the data controller for the purposes of the UK GDPR and the Data Protection Act 2018. The agreed DPA will reflect legislative requirements and obligations but will go beyond this by setting out the ways in which we intend to work together to ensure compliance with the UK GDPR and other relevant legislation. We are flexible on the format of the DPA. We have numerous templates we have used before, but we are happy to use client templates if preferred.

- **Data Subject requests.** At the beginning of any programme, we will agree with our client how we will handle any request from a data subject to exercise any of their rights relating to receiving privacy information, access, rectification, deletion and portability of personal data. This will then be documented

in our DPA. Since we generally act as a data processor on our client programmes (with the client being the data controller), most clients prefer that we refer any request from a data subject to exercise their rights to them as soon as practicable. We have robust internal processes to ensure that this happens, including training for all relevant staff and a reporting process. We then work with our client to determine if any further action is required by us. For example, whether certain data needs to be deleted from our network, in which case our IT team would perform a search of our network and securely delete any relevant records. Where we act as a data controller, our internal systems ensure that we comply with the rights of data subjects and action any subject access request, rectification, deletion or portability request promptly.

- **Data minimisation.** We keep data requirements under constant review and practice the principle of data minimisation at all times. We will not ask for data that we don't need to complete the programme and we won't keep data for longer than we need it. We build data reviews into our programme plans to ensure that we are constantly challenging what data we need and the format in which we need it (for example, can the same analysis be done/outcome achieved with anonymised or pseudonymised data? Does data need to be transferred to Newton, or can the analysis be done on client machines?). If we do process personal data as part of the programme, we will either return it or securely destroy it when we no longer need it.