POLICY

Internal Data Protection Policy

Issued: April 2023
Version: 1.6

Variation
This document replaces the previous Data Protection Policy v1.5 and has been reviewed as part of ICAEW annual compliance procedure. The contents have been updated in this version.

This policy is applicable to ICAEW employees in the *UK only* and does not include staff in our non-UK offices.

CONTENTS

1 Policy statement

1.1 The Institute of Chartered Accountants in England and Wales (**ICAEW**) is committed to ensuring that an appropriate policy is laid down for the internal management and use of Personal Data within the organisation.

1.2 You must read this policy because it gives important information about:

- the data protection principles with which ICAEW must comply;
- what is meant by Personal Data and Special Categories of Personal Data;
- how we gather, use and (ultimately) delete Personal Data and Special Categories of Personal Data in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g., about the Personal Data we gather and use about you, our members or third parties, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

2 Introduction

2.1 ICAEW obtains, keeps and uses Personal Data about a number of individuals, for example:

2.1.1 Job applicants, current and former employees, workers and agency staff, contractors and consultants, apprentices, interns, and people doing work experience;

2.1.2 ICAEW members, including reciprocal and affiliate members;

2.1.3 ICAEW students;

2.1.4 Those working at ICAEW Authorised Training Employers who oversee, and are involved in, the training process;

2.1.5 Pension fund members;

2.1.6 Regulated, assured, registered, licensed and authorised individuals;

2.1.7 Members of ICAEW online communities and forums;

2.1.8 Attendees/Delegates/Trainers at training sessions, webinars and other events;

2.1.9 Suppliers, clients and their employees and other third parties;

2.1.10 Individuals that bring a complaint about an ICAEW member, student, or regulated firm or individual;

2.1.11 Members of the general public browsing the website;

2.1.12 Academics receiving research funding from ICAEW;

2.1.13 Board and Committee Members and volunteers; and

2.1.14 Subscribers to faculties and special interest groups.

2.2 The specific lawful purposes, for which ICAEW obtains, keeps and uses Personal Data are set out in ICAEW's record of processing activities and in ICAEW's privacy notices and associated documents which are provided to individuals when we collect and use their Personal Data.

2.3 This policy sets out how we comply with our data protection obligations and seek to protect Personal Data. Its purpose is also to ensure that all individuals understand and comply with the rules governing the collection, use and deletion of Personal Data to which they may have access in the course of their work.

2.4 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use Personal Data, and how (and when) we delete that information once it is no longer required.

2.5 Our Data Protection Office and our Data Protection Officer are responsible for informing and advising ICAEW and its individuals who have access to Personal Data on its data protection obligations, and for monitoring compliance with those obligations and with ICAEW's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the Data Protection Office via email using: dataprotection@icaew.com.

3 Scope

3.1 This policy applies to all employees of ICAEW, including workers, consultants, contractors and agency staff.

3.2 We will review and update this policy annually.

4 Definitions

criminal records information	means Personal Data relating to criminal convictions and offences, allegations, proceedings, and related security measures.

data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
DPO	means our Data Protection Officer, who is the individual with specific responsibility for data protection in ICAEW.
Personal Data	means information relating to a living individual who can be identified (directly or indirectly) from that information.
Processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with Personal Data.
pseudonymised	means the process by which Personal Data is Processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the Personal Data cannot be attributed to an identifiable individual.
ROPA	our record of processing activities which sets out details of what information we collect, who it is shared with and why.
special categories of personal data	(sometimes known as 'special personal data' or 'sensitive personal data') means Personal Data about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

5 Data protection principles

5.1 ICAEW will comply with the following data protection principles when Processing Personal Data:

5.1.1 we will process Personal Data **lawfully, fairly and in a transparent manner**, for example we will always tell individuals how we collect and use their

Personal Data in privacy notices, and we will make sure that we have a legal basis (condition) for collecting and using their Personal Data;

5.1.2 we will collect Personal Data for **specified, explicit and legitimate purposes** only, and will not process it in a way that is incompatible with those legitimate purposes;

5.1.3 we will only process **Personal Data that is adequate, relevant and necessary** for the relevant purposes;

5.1.4 we will keep **accurate and up-to-date Personal Data**, and take reasonable steps to ensure that inaccurate Personal Data are deleted or corrected without delay;

5.1.5 we will **keep Personal Data for no longer than is necessary** for the purposes for which the information is processed; and

5.1.6 we will take **appropriate technical and organisational measures** to ensure that Personal Data are kept secure and protected against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

6 Legal basis (conditions) for Processing Personal Data

6.1 In relation to any Processing activity, we will, before the Processing starts for the first time, and then regularly while it continues:

6.1.1 review the purposes of the particular Processing activity, and select the most appropriate lawful basis (or bases) for that Processing, i.e.:

(a) that the individual has **consented** to the Processing;

(b) that the Processing is **necessary for the performance of a contract** to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract;

(c) that the Processing is necessary for **compliance with a legal obligation** to which ICAEW is subject;

(d) that the Processing is necessary for the protection of the **vital interests** of the individual or another natural person;

(e) that the Processing is necessary for the performance of a **task carried out in the public interest** or exercise of official authority; or

(f) that the Processing is necessary for the purposes of **legitimate interests** of ICAEW or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the individual – see section 6.2 below.

6.1.2 except where the Processing is based on consent, satisfy ourselves that the Processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose);

6.1.3 document our decision as to which lawful basis applies in our ROPA, to help demonstrate our compliance with the data protection principles;

6.1.4 include information about both the purposes of the Processing and the lawful basis for it in our relevant privacy notice(s);

6.1.5 where special categories of Personal Data are processed, also identify a lawful special condition for Processing that information (see section 7.1.2 below), and document it in our ROPA; and

6.1.6 where criminal offence information is processed, also identify a lawful condition for Processing that information, and document it in our ROPA.

6.2 When determining whether ICAEW's legitimate interests are the most appropriate basis for lawful Processing, we will:

6.2.1 conduct a legitimate interest assessment (**LIA**) and keep a record of it, to ensure that we can justify our decision;

6.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (**DPIA**);

6.2.3 keep the LIA under review, and repeat it if circumstances change; and

6.2.4 include information about our legitimate interests in our relevant privacy notice(s).

7 Special Categories of Personal Data

7.1 We may from time to time need to process Special Categories of Personal Data. For more detail of how we process Special Categories of Personal Data please see the specific Appropriate Policy Document relating to the use of the Personal Data in that way. We will only process Special Categories of Personal Data if:

7.1.1 we have a lawful basis for doing so as set out in section 6.1.1 above, e.g., it is necessary for the performance of the employment contract, to comply with ICAEW's legal obligations or for the purposes of ICAEW's legitimate interests; and

7.1.2 one of the special conditions for Processing Special Categories of Personal Data applies, e.g.:

(a) the individual has given **explicit consent**;

(b) the Processing is necessary for the purposes of **exercising the employment law rights or obligations** of ICAEW or the individual;

(c) the Processing is necessary to protect the individual's **vital interests**, and the individual is physically incapable of giving consent;

(d) Processing relates to Personal Data which are **manifestly made public by the individual**;

(e) the Processing is necessary for the e**stablishment, exercise or defence of legal claims**;

(f) the Processing is necessary for **reasons of substantial public interest**; or

(g) we have a lawful basis for doing so under the **Data Protection Act 2018**.

7.2 Before Processing any Special Categories of Personal Data, individuals must notify the Data Protection Office of the proposed Processing, in order that we may assess whether the Processing complies with the criteria noted above.

7.3 Special Categories of Personal Data will not be Processed until:

7.3.1 the assessment referred to in section 7.2 has taken place; and

7.3.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the Processing, the purposes for which it is being carried out and the legal basis for it.

7.4 ICAEW will not carry out automated decision-making (including profiling) based on any individual's Special Categories of Personal Data.

7.5 ICAEW's privacy notices set out the types of Special Categories of Personal Data that ICAEW processes, what it is used for and the lawful basis for the Processing.

7.6 In relation to Special Categories of Personal Data relating to employees and other personnel, ICAEW will comply with the procedures set out in section 7.6.1 and section 7.6.2 below to make sure that it complies with the data protection principles set out in section 5 above.

7.6.1 **Employees and other personnel – during the recruitment process**: the HR team, with guidance from our Data Protection Office will ensure that (except where the law permits otherwise):

(a) during the short-listing, interview and decision-making stages, no questions are asked relating to Special Categories of Personal Data, e.g., race or ethnic origin, trade union membership or health except where it is necessary to ask questions about a candidate's health or disability, in order to make reasonable adjustments to the interview and selection process, or to employment arrangements because of a candidate's disability;

(b) if Special Categories of Personal Data are received, e.g., the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

(c) any completed equal opportunities monitoring form is kept separate from the individual's application form, and will not be seen by the person shortlisting, interviewing or making the recruitment decision. The form will however be seen by HR Recruitment in order that they can assess if any reasonable adjustments need to be made to the interview and selection process, or to employment arrangements because of a candidate's disability;

(d) 'right to work' checks are carried out after an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages; and

(e) we will only ask health questions once an offer of employment has been made, except where it is necessary to ask questions about a candidate's health or disability, in order to make reasonable adjustments to the interview and selection process, or to employment arrangements because of a candidate's disability.

7.6.2 **Employees and other personnel – during employment**: the HR team, with guidance from our Data Protection Office will process:

(a) health information for the purposes of administering sick pay, keeping sickness absence records, monitoring individual's attendance, assessing and facilitating any additional assistance to the employee based on their health needs and facilitating employment-related health and sickness benefits;

(b) Special Categories of Personal Data for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised.

8 Criminal records information

We may from time to time need to process Personal Data relating to criminal records. For more detail of how we process Personal Data relating to criminal records please see the specific Appropriate Policy Document relating to the use of Personal Data in that way.

9 Data protection impact assessments (DPIAs)

9.1 Where Processing is likely to result in a high risk to an individual's data protection rights we will, before commencing the Processing, carry out a DPIA to assess:

9.1.1 whether the Processing is necessary and proportionate in relation to its purpose;

9.1.2 the risks to individuals; and

9.1.3 what measures can be put in place to address those risks and protect Personal Data.

9.2 Before all new projects involving a new collection of Personal Data, new data sharing or where Personal Data is going to be used for a new purpose you must complete the DPIA Checklist to determine whether a DPIA is required. This is in compliance with our DPIA Policy.

9.3 During the course of any DPIA, ICAEW will seek the advice of our Data Protection Office and/or the DPO and the views of a representative group of employees and any other relevant stakeholders.

10 Documentation and records

10.1 We have a ROPA to record our data Processing activities. This contains information relating to the following matters:

10.1.1 the identity of the controller, processor or joint controller;

10.1.2 details of any data protection officer for the relevant controller, processor or joint controller;

10.1.3 the purposes of the Processing;

10.1.4 a description of the categories of individuals and categories of Personal Data;

10.1.5 categories of recipients of Personal Data;

10.1.6 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;

10.1.7 where possible, retention schedules; and

10.1.8 where possible, a description of technical and organisational security measures.

10.2 As part of our ROPA we document, or link to documentation, on:

10.2.1 information required for privacy notices;

10.2.2 records of consent;

10.2.3 controller-processor contracts;

10.2.4 the location of Personal Data; and

10.2.5 DPIAs.

10.3 When we process Special Categories of Personal Data or Criminal Records Information, we will keep written records of:

10.3.1 the relevant purpose(s) for which the Processing takes place, including (where required) why it is necessary for that purpose;

10.3.2 the lawful basis for our Processing; and

10.3.3 whether we retain and erase the Personal Data in accordance with our Data Retention and Destruction Policy and, if not, the reasons for not following our Data Retention and Destruction Policy.

10.4 We will conduct regular reviews of the Personal Data we process and update our documentation accordingly. This may include:

10.4.1 carrying out information audits to find out what Personal Data ICAEW holds;

10.4.2 distributing questionnaires and talking to individuals across ICAEW to get a more complete picture of our Processing activities; and

10.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

11 Privacy notices

11.1 ICAEW will issue privacy notices, informing individuals about the Personal Data that we collect and hold, how individuals can expect their Personal Data to be used and for what purposes. These privacy notices will be provided at the point of data collection or as soon as we use the Personal Data, if this has come from another source, for example, if we ever use Personal Data passed to us by a third party for example, a member firm or marketing agency.

11.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

12 Individuals' rights

12.1 Individuals (this includes our employees and members) have legal rights in relation to their Personal Data.

12.1.1 **The right to be informed**

(a) Individuals have a right to be informed about how we will use and share their Personal Data, we provide this information in a clear and transparent manner in our privacy notices.

12.1.2 **The right of access**

(a) Individuals have the right to know if we are Processing their Personal Data and access to their Personal Data along with additional pieces of information, for example, who this is shared with.

(b) We do not always have to provide all the information if exemptions apply.

12.1.3 **The right to rectification**

(a) Individuals have a right to have any inaccurate or incomplete Personal Data rectified.

(b) If we have passed this data to any third parties, we have an obligation to also inform them that we have received this request, unless it is disproportionate to do so.

12.1.4 **The right to erasure (also known as the "right to be forgotten")**

(a) In certain circumstances, individuals have a right to request that Personal Data held by us is erased.

(b) If we have passed this data to any third parties, we have an obligation to also inform them that we have received this request, unless it is disproportionate to do so.

(c) This right applies if we:

(i) process Personal Data beyond the period when it is necessary to do so for the purpose for which it was originally collected;

(ii) rely on consent and the individual withdraws their consent;

(iii) rely on legitimate interests and the individual objects and there is no overriding compelling ground which enables us to continue Processing the Personal Data; or

(iv) are Processing the Personal Data unlawfully (i.e., in breach of the requirements of the UK GDPR).

12.1.5 **The right to restrict Processing**

(a) In certain circumstances, individuals have the right to restrict the Processing of their Personal Data.

(b) If we have passed this data to any third parties, we have an obligation to also inform them that we have received this request, unless it is disproportionate to do so.

(c) This right applies, if:

(i) an individual disputes the accuracy of Personal Data;

(ii) an individual has raised an objection to the Processing of Personal Data;

(iii) the Processing of Personal Data is unlawful, and the individual opposes erasure and requests restriction instead; or

(iv) the Personal Data is no longer required by us but the individual requires the Personal Data to be retained to establish, exercise or defend a legal claim.

12.1.6 **The right to data portability**

(a) In certain circumstances, individuals have a right to obtain and reuse Personal Data that they have provided to us for their own purposes across different services.

(b) This right only applies to Personal Data that the individual has provided to us and when we are Processing the Personal Data based on consent or for the performance of a contract and we are carrying out the Processing by automated means.

12.1.7 **The right to object**

(a) In certain circumstances, individuals have the right to object to the Processing of their Personal Data.

(b) They have an absolute right to stop their data being used for direct marketing.

(c) We must tell individuals about their right to object, separately from other information on their rights. We must do this by, for example, including this information clearly in privacy notices and on direct marketing communications; and

12.1.8 **Rights in relation to automated decision making and profiling**

(a) Individuals have a right not to be subject to a decision which is based on automated Processing where the decision will produce a legal effect or a similarly significant effect on the individual for example, a decision whether to enter into a contract with an individual, decisions

in relation to whether credit will be extended to an individual and decisions to cut off a supply.

(b) If we undertake automated decision-making including profiling, we must:

(i) provide individuals with information about the Processing;

(ii) introduce easy ways for them to request human intervention or challenge a decision; and

(iii) carry out regular checks to make sure that our systems are working as intended and are producing the right outcomes.

12.2 If you receive a request from an individual to exercise any of the rights detailed above, you must notify the Data Protection Office as soon as possible.

12.3 We must respond to all rights requests without undue delay and in any event within **one calendar month** of receipt of the request . This period may be extended by a further two months, where necessary, taking into account the complexity of the request. **All requests to extend the one-month period must be approved by our Data Protection Office.**

13 Our obligations

13.1 All individuals are responsible for helping ICAEW keep Personal Data up to date. You should let the HR team know if the Personal Data you have provided to ICAEW changes, for example if you move to a new house or change details of the bank or building society account to which you are paid.

13.2 You may have access to the Personal Data of other employees, suppliers and members and other third parties of ICAEW in the course of your employment or engagement. If so, ICAEW expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in section 12 above.

13.3 If you have access to Personal Data, you must:

13.3.1 only access the Personal Data that you have authority to access, and only for authorised purposes;

13.3.2 only allow other individuals to access Personal Data if they have appropriate authorisation;

13.3.3 only allow individuals who are not authorised individuals to access Personal Data if you have specific authority to do so from your Managing Director;

13.3.4 keep Personal Data secure (e.g., by complying with rules on access to premises, computer access, password protection and secure file storage and

destruction and other precautions set out in ICAEW's Information Security Policy);

13.3.5 not remove Personal Data, or devices containing Personal Data (or which can be used to access it), from ICAEW's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

13.3.6 not store Personal Data on local drives or on personal devices that are used for work purposes and comply with ICAEW's Information Security Policy.

13.4 You should contact our DPO if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

13.4.1 Processing of Personal Data without a lawful basis for its Processing or, in the case of Special Categories of Personal Data, without one of the conditions in section 7.1.2 being met;

13.4.2 any Data Breach as set out in section 16.1 below;

13.4.3 access to Personal Data without the proper authorisation;

13.4.4 Personal Data not kept or deleted securely;

13.4.5 removal of Personal Data, or devices containing Personal Data (or which can be used to access it), from ICAEW's premises without appropriate security measures being in place; and

13.4.6 any other breach of this policy or of any of the data protection principles set out in section 5.1 above.

14 Information security

14.1 ICAEW will use appropriate technical and organisational measures in accordance with ICAEW's Information Security Policy to keep Personal Data secure, and in particular to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage. These may include:

14.1.1 making sure that, where possible, Personal Data is pseudonymised or encrypted;

14.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

14.1.3 ensuring that, in the event of a physical or technical incident, availability and access to Personal Data can be restored in a timely manner; and

14.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

14.2 Where ICAEW uses external organisations to process Personal Data on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of Personal Data. In particular, contracts with external organisations must provide that:

14.2.1 the organisation may act only on the written instructions of ICAEW;

14.2.2 those Processing the data are subject to a duty of confidence;

14.2.3 appropriate measures are taken to ensure the security of Processing;

14.2.4 sub-contractors are only engaged with the prior consent of ICAEW and under a written contract;

14.2.5 the organisation will assist ICAEW in providing subject access and allowing individuals to exercise their rights in relation to data protection;

14.2.6 the organisation will assist ICAEW in meeting its obligations in relation to the security of Processing, the notification of data breaches and data protection impact assessments;

14.2.7 the organisation will delete or return all Personal Data to ICAEW as requested at the end of the contract; and

14.2.8 the organisation will submit to audits and inspections, provide ICAEW with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell ICAEW immediately if it is asked to do something infringing data protection law.

14.3 Before any new agreement involving the Processing of Personal Data by an external organisation is entered into, or an existing agreement is altered, the relevant individual must seek approval of its terms from the legal team, and you must follow ICAEW's Third Party Contracts and Agreements Policy.

15 Storage and retention of Personal Data

15.1 Personal Data (and Special Categories of Personal Data) will be kept securely in accordance with ICAEW's Information Security Policy.

15.2 Personal Data (and Special Categories of Personal Data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the Personal Data was obtained.

15.3 Individual's must follow ICAEW's Data Retention and Destruction Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period.

15.4 Where there is any uncertainty, individuals should consult our Data Protection Office.

15.5 Personal Data (and Special Categories of Personal Data) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

16 Data breaches

16.1 A Data Breach may take many different forms, for example:

16.1.1 loss or theft of data or equipment on which Personal Data is stored;

16.1.2 unauthorised access to or use of Personal Data either by an employee or third party;

16.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

16.1.4 human error, such as accidental deletion or alteration of data;

16.1.5 unforeseen circumstances, such as a fire or flood;

16.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

16.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

16.2 ICAEW will:

16.2.1 make the required report of a Data Breach to the Information Commissioner's Office (**ICO**) without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

16.2.2 notify the affected individuals if a Data Breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16.3 **If you suspect any Data Breaches, no matter how small you must report these immediately to our Data Protection Office** and you must follow our Data and Cyber Incident Management Policy.

17 Training

ICAEW will ensure that individuals are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to Personal Data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 International transfers

18.1 ICAEW may transfer personal information outside the United Kingdom provided that the country, territory or organisation is designated as having an adequate level of protection or that the organisation receiving the information has provided adequate safeguards by way of binding corporate rules or standard data protection clauses.

19 Consequences of failing to comply

19.1 ICAEW takes compliance with this policy very seriously. Failure to comply with the policy:

19.1.1 puts at risk the individuals whose Personal Data is being processed; and

19.1.2 carries the risk of significant civil and criminal sanctions for the individual and ICAEW and

19.1.3 may, in some circumstances, amount to a criminal offence by the individual.

19.2 Because of the importance of this policy, an individual's failure to comply with any requirement of it may lead to disciplinary action. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

19.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact our Data Protection Office.

20 Associated Policies

20.1 The following ICAEW policies are associated with this policy.

20.1.1 Information Security Policy

20.1.2 Data Protection Impact Assessment Policy

20.1.3 Electronic Communications and Monitoring Policy

20.1.4 Data Retention and Destruction Policy

20.1.5 Appropriate Policy Document

20.1.6 PCI DSS Policy

20.1.7 Bring You Own Device Policy

20.1.8 Data and Cyber Incident Management Policy

These policies can be found on the Intranet at ICAEW Policies

Document control

Date: April 2023
Expiry: April 2024
Confidentiality: ICAEW use only
Version: 1.6
Owner: Data Protection Office
Drafted by: HelloDPO Ltd and Helen Carter, Data Protection Office
Approved by: Data Protection Oversight Group
Next review date: April 2024
Linked documents: None.