FUTURE-PROOF BANK

We are committed to providing positive experiences for all our customers, learning from our mistakes and putting things right when they go wrong. In an increasingly digitalised world, we're continuing to invest in the resilience of our business, areas such as cyber security and data ethics are of fundamental importance to us.

THIS CHAPTER COVERS OUR RESPONSE TO THE FOLLOWING MATERIAL TOPICS:

- → CUSTOMER EXPERIENCE
- → DIGITALISATION AND INTERCONNECTIVITY
- → CYBER SECURITY AND BUSINESS SYSTEM RESILIENCE
- → PROTECT OUR CUSTOMERS' DATA AND PRIVACY
- → CORPORATE GOVERNANCE AND ACCOUNTABILITY
- → ETHICS AND INTEGRITY
- → COMPLY WITH LAWS, CODES AND REGULATIONS
- → TALENT ATTRACTION AND RETENTION

OUR PROGRESS IN 2020

MATERIAL TOPICS

CUSTOMER EXPERIENCE

66,000 COVID PAYMENT BREAKS OFFERED

PAYMENT BREAK **NPS +62**

80,000 VOICE OF THE CUSTOMER SURVEYS COMPLETED

DIGITALISATION AND INTERCONNECTIVITY

OVER 80% ENABLED TO WORK REMOTELY

NEW ONLINE STANDARD FINANCIAL STATEMENT

CYBER SECURITY AND BUSINESS SYSTEM RESILIENCE

ONGOING CYBERSECURITY TRAINING

DATA GOVERNANCE ENHANCEMENTS

PROTECT OUR CUSTOMERS' DATA AND PRIVACY

NEW DATA ETHICS **PRINCIPLES**

DATA STORAGE MODERNISATION

CORPORATE GOVERNANCE AND ACCOUNTABILITY

MULTI YEAR **CULTURE EVOLUTION PROGRAMME**

REFRESHED **VALUES** LAUNCHED

ETHICS AND INTEGRITY

ENHANCED CODE OF CONDUCT

NEW SUPPLIER CODE

COMPLY WITH LAWS, CODES AND REGULATIONS

1,374 PARTICIPATED IN RISK **AWARENESS WEEK**

FIRST BANK TO LAUNCH THE RIGHT TO **DISCONNECT**

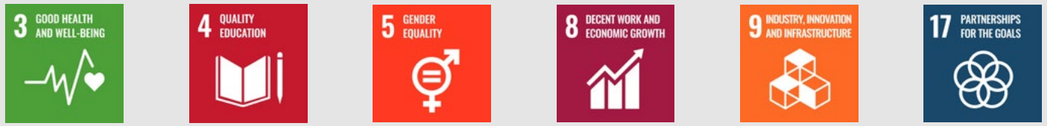
HUMAN RIGHTS COMMITMENT PUBLISHED

TALENT ATTRACTION AND RETENTION

5,000 PARTICIPATE IN **INVEST IN YOU**

857 EMPLOYEES GAIN INSTITUTE OF BANKING **AWARDS**

SUSTAINABLE DEVELOPMENT GOALS



We pledge to **DO MORE.**

AIB Sustainability

CUSTOMER EXPERIENCE

OUR APPROACH

Our customers' feedback and experiences inform and guide us, helping us to focus on our actions so that we can provide them with the best banking experiences.

As the pandemic impacted our economies, we moved quickly to give help where it mattered most, putting in place a comprehensive COVID-19 customer support programme. Unfortunately, previously planned changes to fees and charges took effect for some of our customers just as they were trying to manage the immediate impact of COVID-19. The timing of their introduction had an unintended impact for some of these customers, however as soon as we realised we moved quickly to put it right for them. Our COVID-19 customer support programme included offering over 66,000 payment breaks, which were made available to our Homes, SME and Personal customers in 2020.

We understand that buying a home is a significant milestone for many customers. In Ireland, we have a team of specialist home advisors who can assist and will meet at a time and place which is convenient for our customers. In 2020, we introduced some new online functionality to enhance the customer experience. Whether customers start applying for a mortgage with us in branch or online they can use our My Mortgage app to upload the documents needed for us to assess the application, and to track the progress of their loan. In addition, since 2020, customers in mortgage arrears can now fill out and submit a Standard Financial Statement (SFS) securely online (see p.70). By completing their SFS more quickly, this increases the speed at which they can be offered a sustainable solution to their financial difficulty.

LISTENING TO OUR CUSTOMERS

We listen to our customers to learn from their experience with our business. We monitor customer satisfaction using Net Promoter Score (NPS). NPS is an index ranging from -100 to 100 that measures the willingness of customers to recommend a company's products/services to others.

The range of initiatives we used in 2020 to engage with all our stakeholders are set out on p.18-21. Specifically, for our customers, a key engagement mechanisms was our Voice of the Customer (VOC) programme. 80,000 customers completed our VOC surveys in 2020. The programme gives our customers the opportunity to tell us what we are doing well and where we can do better.

A recent NPS survey on the Payment Break Experience highlighted an NPS score of +62 (+55 for EBS), with 69% (66% EBS) giving a 9/10 promoter score. COVID-19 communications have been issued to c. 70,000 customers with the vast majority either agreeing or strongly agreeing that the communications were clear, easy to understand, helpful, and supportive.

COMPLAINTS

We see complaints as a valuable way for our customers to let us know if they are unhappy with what we have done or failed to do. We listen to and empathise with our customers to understand and resolve complaints as effectively as possible. Understanding our customers better means, in most cases, we can reach a satisfactory conclusion for both them and us. Acknowledging how our mistakes can affect our customer's lives and working hard to resolve them helps to build trust. We have a Complaints Management policy in place setting out responsibilities for managing complaints, and a Complaints Management System to log, monitor and update complaints and a centralised team to support complex complaints.

There have been times when we haven't gotten things right for our customers. When we do not get it right first time, our priority always is to put things right.

COVID-19 RISK RESPONSE

In March, our Risk area established a COVID-19 Risk Response team. This team supported the co-ordination and management of the Group's response to the pandemic to ensure business continuity for our employees, customers and investors.

In recognition of the significant volume of Risk function activities to be delivered in a compressed timeframe, and to ensure delivery of a co-ordinated 'One Risk' response, critical work streams and enhanced business as usual activities were supported and enabled by a formal Risk COVID-19 programme. These included the Risk review and challenge of the design and development of payment breaks across our product offerings for customers impacted by COVID-19. The purpose of these reviews was to ensure potential risks associated with the product offerings were quickly identified, assessed and addressed prior to making them available to our customers.

Furthermore, an Assurance team was mobilised to perform independent assurance on customer solutions to ensure they were fit for purpose for our customers and implemented appropriately in our business. Almost 14,000 applications in Ireland and a further 5,000 in the United Kingdom were tested as part of this assurance exercise.

Across Risk, policies, processes and business activities were required to rapidly adapt to support our response to COVID-19 and to ensure minimal impact on our customers and our business. Examples of how we improved our services and customer experiences to support our customers include:

- a Credit Risk Management work stream was mobilised to manage the rapidly changing credit risk environment and activities, to ensure our employees on the frontline could help our customers businesses respond in the face of COVID-19
- the EBS Mortgage Lending Unit modified existing processes to ensure they could provide mortgage payment breaks to EBS customers – a solution which was not available prior to COVID-19
- a Fraud/AML work stream mobilised in Ireland to manage the enhanced oversight activity due to changes implemented in AIB product offerings
- changes to our Property Valuations policy and processes were implemented to adapt during the period when valuers were unavailable to provide external valuations.

CUSTOMER EXPERIENCE

VOICE OF THE CUSTOMER NET PROMOTER SCORE (NPS)

The Voice of the Customer (VOC) programme collects feedback from c. 20,000 customers per quarter who tell us where we provide great customer experience and how we can improve our products, services and delivery channels using NPS.

In 2020 over 80,000 customers completed our VOC surveys and had the opportunity to tell us how we were performing across our customer journeys. In addition, we also measured over 30,000 of our customer's digital interactions via a range of intercept surveys. We listen to our customers to learn from where we delivered exceptional experiences and also continuously analyse the root causes of customer pain points to ensure we enhance our customer's experiences when we don't meet their expectations.

The pandemic brought some challenges in terms of how we could support customers during difficult times. Encouragingly, the majority of our customer journeys increased in 2020 continuing the trend we saw in 2019. 11 customer journeys have shown an improvement in 2020, 6 have remained stable and 4 journeys have declined as we adjusted to the changing macro environment. COVID-19 placed additional demands on our employees, and alongside a necessary focus on regulatory changes, there were initial impacts on a small number of the day-to-day support customers received. This was addressed through adaptation of employees and process to the new environment.

Our Retail SME customers have been very positive about their experiences with us in 2020 with Retail SME Relationship NPS increasing by +5 and the Retail SME Transactional NPS also increasing by +5 vs 2019. Our teams across Retail SME certainly made our customers feel valued and were there for them when needed with the right solutions.

- Personal customers have told us that there are areas we can improve on with negative sentiment around fees & charges and the inability for some or our customers to contact and engage in our channels on the back of the pandemic, resulting in the Personal Relationship NPS declining by -9 vs 2019.

- NPS for 13 of our transactional journeys was +60 or above in 2020, with significant increases in the mortgage journeys of EBS Mortgage Drawdown and AIB Mortgage Decline and the credit journeys of Credit Card and Cashflow.

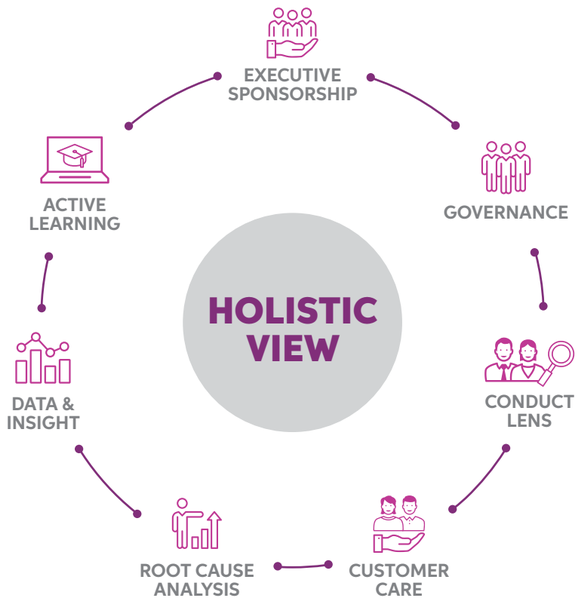
CUSTOMER THEMES

Positive themes mentioned by customers for our overall NPS improvement include employee helpfulness, attitude and professionalism and ease of using our more secure digital services. However in completing day-to-day digital banking as a result of secure customer authentication has frustrated a minority of customers. Other negative themes mentioned by customers focus around changes in credit policy and high fees and charges.

CUSTOMER EXPERIENCE

MANAGING CUSTOMER COMPLAINTS

We adopt a holistic approach to achieving better customer outcomes, with a focus on proactive consumer protection throughout the product/ service lifecycle. Notwithstanding our focus on Conduct, we know that from time to time things will go wrong. When they do, customers can use our complaints handling process to tell us about it.



We work to handle complaints speedily, efficiently and fairly. We have a formal complaints handling process and procedure in place. When we receive a complaint from a customer we respond and give details of a dedicated contact person who will manage the complaint. Our processes differentiate between complex and less complex complaints, with our business areas managing and addressing the more straightforward complaints while complex complaints are increasingly addressed centrally in our Customer Care Centre of Excellence (CCL), which is based in Limerick.

We are constantly seeking out ways we can improve how we manage customer complaints, looking at both the processes in place to manage complaints and via analysis of the underlying issues which may have given rise to the complaint in the first instance. In 2016 we began centralising the management of complex complaints and over the course of 2020 we further extended the reach of CCL by integrating our Investment & Protection complaints function and began the transfer of complex complaint handling from our EBS offices.

We listen to and empathise with customers to understand and resolve complaints as effectively as possible. Understanding our customers better means, in most cases, we can reach a fair and satisfactory outcomes for our customer. We endeavour to resolve all customer complaints within 40 days and if this is not possible we advise the customer of the expected time frame to closure.

Despite the impact of the COVID-19 pandemic in 2020, and the resulting changes in our working environment, CCL's customer service delivery continued uninterrupted.

The average time taken to close a complaint during 2020 has been maintained at the 2019 level of 14.5 days – reduced from 27 days in 2015.

We also achieved an improved NPS of -17.6, versus -24.3 in 2019 a 6.7 year on year improvement. Our Limerick Customer Care team won the Gold Award in the Most Improved Complaint Handling (Financial Services) category at the UK Complaint Handling Awards 2020.

FINANCIAL SERVICES & PENSIONS OMBUDSMAN (FSPO)

If a consumer is dissatisfied with how we have closed their complaint they can refer it to the office of the FSPO. We endeavour to address as many complaints as possible using the FSPO's informal dispute resolution process or via mediation. When a complaint progresses to formal investigation stage, we analyse the FSPO decisions and share learnings and insights to improve customer outcomes.

The FSPO team has made significant progress in increasing the number of cases closed using the dispute resolution process, prior to cases moving to the formal investigation stage of the process.

LEVEL OF CASES CLOSED USING THE FSPO DISPUTE RESOLUTION PROCESS

CUSTOMER EXPERIENCE

GROUP CONDUCT

Group Conduct's mission is to promote and sustain a customer centric culture and ensure a conduct lens is applied to all aspects of business, ensuring that the conduct risks inherent in the bank's activities are identified, managed, and monitored to allow us to grow in a sustainable manner and deliver on our Customer First ambition.

Our Group Conduct Committee together with divisional segment committees have responsibility for our consumer protection agenda. Group Conduct's objective is to promote and sustain a customer centric culture and apply a conduct lens to all aspects of our business, ensuring that the conduct risks inherent in our activities are identified, managed and monitored to allow us to grow in a sustainable manner and deliver on our Customer First ambition. The way in which we achieve this is to maintain a sustained focus on conduct risk management effectiveness across the Bank through training and guiding business areas to both proactively identify and measure their conduct risk exposure thereby enabling its effective control.

Our Group conduct strategy is supported by annual business segment conduct action plans, delivering against key strategic objectives, ensuring continued progress on embedding conduct and meeting evolving regulatory expectations.

Conduct risk for AIB is the risk that inappropriate actions or inactions cause poor and unfair customer outcomes. For example, customer complaints outstanding without proper investigation would lead to unfair customer outcomes. We have a Conduct Risk Framework, which is embedded in the organisation and provides oversight at Executive and Board level via our Group Conduct Committee and the Group Product and Proposition Committee. To support this, a suite of policy standards, including a Group Conduct risk policy clearly define expected standards of behaviour, including how we lend responsibly and how we support our vulnerable customers. Our Group Head of Conduct and team provides independent oversight and governance of conduct risk across AIB and is a mandatory approver of product/ propositions proposals.

Segment Conduct Committees, operating to standard terms of reference, actively drive the conduct agenda and manage conduct risk within their businesses. All employees must complete Code of Conduct training, and bespoke conduct training was provided to 350 employees in 2020.

We measure key management information trends aligned with the business conduct action plans in our segment conduct dashboard.

CONDUCT TRAINING WAS DELIVERED TO **c. 350** EMPLOYEES

77 PRODUCT & CUSTOMER SOLUTION REVIEWS

TRACKER MORTGAGE EXAMINATION

In terms of legacy issues, last year we completed payments to c. 5,900 customers in relation to the AIB prevailing tracker rate issue and to c. 1,000 EBS customers who were deemed impacted under the Tracker Mortgage Examination (TME) during 2020.

In relation to the AIB prevailing tracker rate issue, c. 5,600 of these customers received the application of a Financial Services and Pensions Ombudsman (FSPO) decision, as well as, following the intervention of the Central Bank of Ireland (CBI), providing TME payments to c. 300 customers who rolled off tracker rates very shortly after trackers were withdrawn and were deemed impacted under the TME.

In terms of the impacted EBS customers, payments were completed to c. 1,000 EBS customers who had been identified as part of the CBI's tracker investigation process.

We will, on an ongoing basis work closely with the CBI in relation to any tracker-related issues and associated enforcement investigations.

Our focus on putting things right for customers has continued and so the correction of these two issues has been a critical priority throughout 2020.

If customers have any queries they can call our AIB dedicated helpline on 1800 235 460 (+353 1 771 5888) or EBS helpline on 1800 235 461 (+353 1 771 5889) between 8am and 7pm Monday to Friday.

DIGITALISATION AND INTERCONNECTIVITY

OUR APPROACH

We are the number one digital bank in Ireland. We have a continuous focus on expanding the accessibility of products and services via our digital channels.

Our approach to digitalisation is to expand our offering in an attractive way to enable our customers to digitally request more and more services. Traditionally, access to our products and services was constrained by opening hours and physical locations, and often defined by paper of voice/call instruction. Through digitalisation and digitisation we can foster agility and flexibility, and ultimately offer our customers much greater accessibility. This provides us with the opportunity to continue the shift from paper in both incoming requests and in the way we communicate with customers. This can mean digitally capturing instructions when face to face with a customer in a branch setting, as well as as enabling an equivalent request via a mobile phone engagement when our customers are at home. Our customers have different preferences, and we maintain a strong culture and framework around customer conduct responsibilities in guiding us as we design and enhance our processes.

BUILDING OUR EXPERTISE

Innovative thinking is critical in enhancing our digital infrastrucutre and digitising customer services, and we have invested in our employees to build their knowledge and expertise in this space. To support the development of strategic leadership in this space, some of our employees have commenced the University of Warwick's Executive Diploma in Digital Leadership programme focused on digital leadership, strategy, innovation and organisational change.

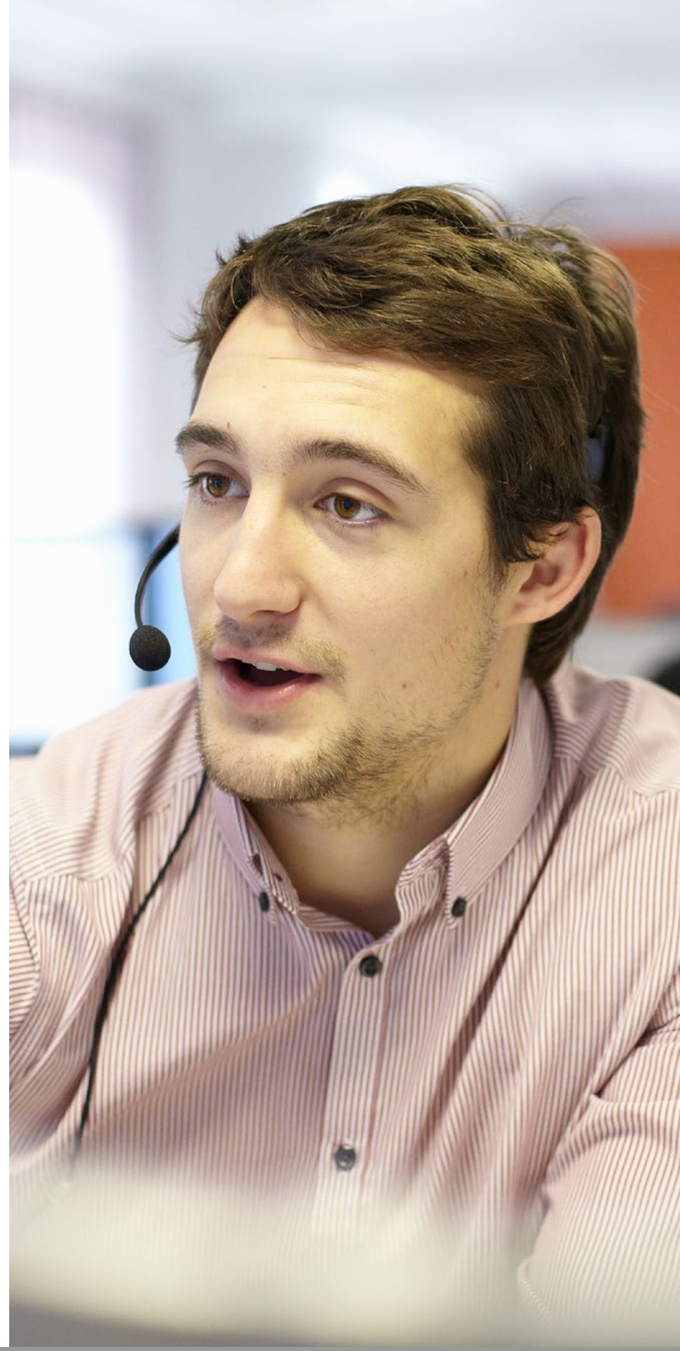
RISK MANAGEMENT

Our Continuity & Resilience and IT Risk policies, components of the Operational Risk Framework, support the management of risks in the availability of our technical infrastructure and digital capability. As we continue to innovate and develop our digital offerings, we maintain focus on the management of third party, cyber and resilience risks to effectively protect the bank and customer data and privacy.

PROGRESS IN 2020 AND LOOKING AHEAD

We are making good progress on this material topic. In 2020 we continued to see a great adoption of electronic statements and advices by our personal customers. The cumulative effect of this switch by our customers led to a reduction in use of more than 14m pages and 5m envelopes. A further key initiative in this space was our Online Standard Financial Statement (see p.70).

In 2021 we will see our enabling of this shift for our business customers, who we recognise are keenly interested in the paperless agenda, and we aim to deliver additional service offerings to them.



DIGITALISATION AND INTERCONNECTIVITY

KEEPING THE BANK CONNECTED – SCALING REMOTE ACCESS

We were well positioned to respond to the increased demands for remote access during the COVID-19 crisis. We had delivered a major internet infrastructure upgrade programme over the previous 18 months, foreseeing a time when the bank would need greater flexibility to handle major Red Weather impacts, and other unforeseen crisis events.

OVER 80% ENABLED TO WORK REMOTELY

COVID-19 necessitated an immediate and widespread move to home working. In a very short timeframe we enabled over 80% of our employees to work remotely.

Whilst the infrastructure was well placed to handle this rapid increase in demand, it was also seamlessly scaled during the crisis. We increased our internet bandwidth by 500% within two hours to handle the varying data transmission needs of employees using remote access.

KEEPING THE BANK COMMUNICATING

During COVID-19 over 2,500 telephony changes were undertaken. These included redirection of individual telephony lines and rapid development of a new trading floor in under 48 hours, and enabling new remote contact centre employee functionality. We now support up to 240 contact centre employees from home every day, with full functionality including call recording. This solution, developed in four weeks, is a significant enhancement to our overall business continuity for a critical front-line service that has experienced significant customer volumes during COVID-19, allowing us to continue to support our customers and employees when they need us most.

NEW TOOLS & COLLABORATION CAPABILITIES

While communications technologies are largely focused on enabling the individual, collaboration technologies are more focused on enabling teams; e.g. voice and video, conferencing, chat, and document-sharing. Our successful enabling of remote working at scale drove a new need to uplift the collaboration capability of our colleagues across the Bank.

We developed a 12 week rapid deployment roadmap and mobilised a team to accelerate delivery of some components of the Digital Workplace programme to achieve the following:

1. Extend current communication solutions, i.e. extend Skype for Business to a broader population
2. Extend our prototype collaboration solutions (i.e. the Mobility Pilot) to specific groups for business-critical collaboration
3. Extend our meeting room video capability to allow office-based colleagues and remote workers to connect on video
4. Making the smartphone smarter; enhancing functionality on our corporate iPhone and iPad fleet
5. Drive sufficient training and adoption to maximise the potential of the technology.

Understandably, the bank's use of conference lines had risen significantly and in response we rapidly expanded Skype for Business and established a WebEx events service for larger scale events calls. In 2021, this will be updated again as Microsoft Teams is rolled out at scale.

DIGITALISATION AND INTERCONNECTIVITY

ONLINE STANDARD FINANCIAL STATEMENT (SFS)

The Online SFS project digitised a paper-based credit restructure process by replacing the paper standard financial statement with a digital form through DocuSign.

Moving to the online SFS has saved customers time as forms can be completed and returned more quickly, increasing the the speed at which they can be offered a sustainable solution to their financial difficulty.

The Online SFS form is available 24/7 via our website, accessible on mobile or desktop, there are also validations built into the form to reduce the chance of mistakes that could result in a delay due to rework.

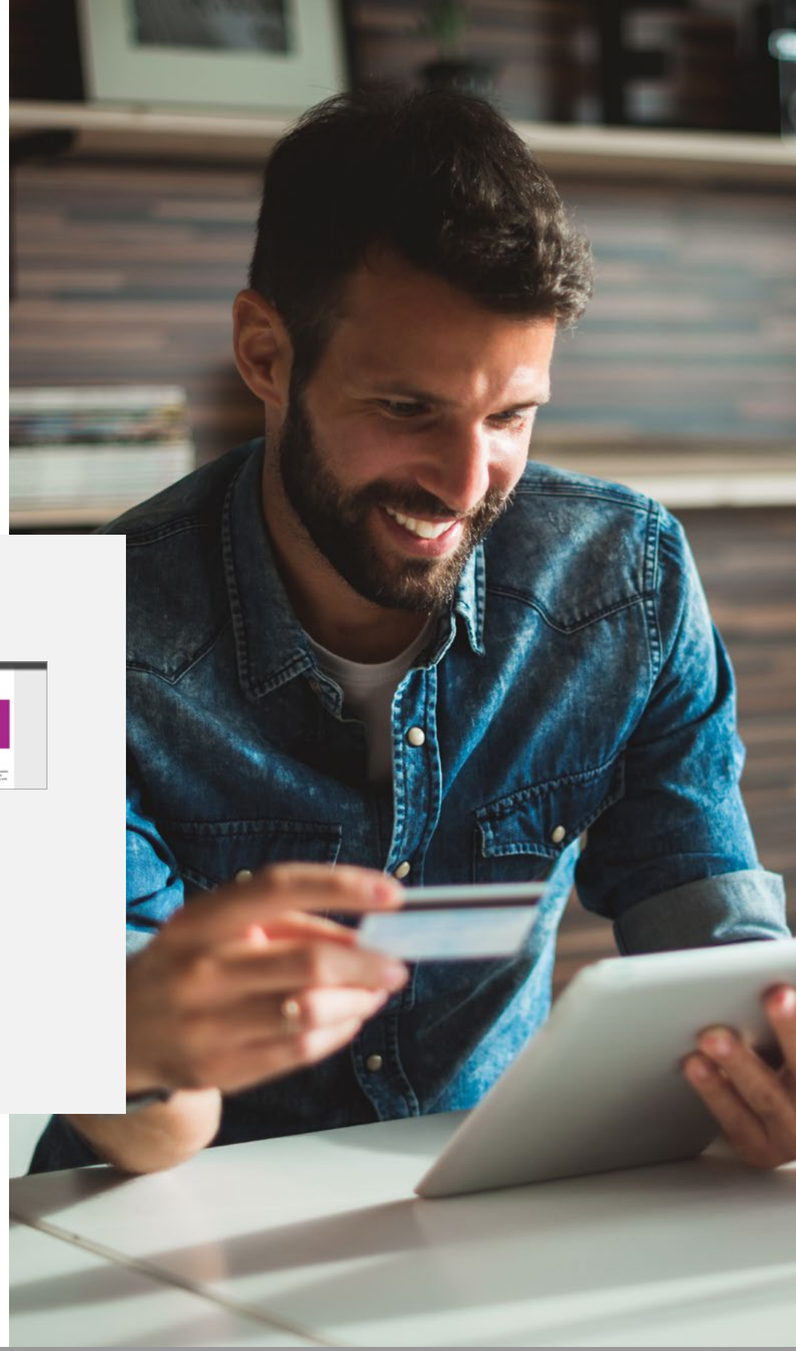
The online solution is accessible to separated borrowers and borrowers represented by third party advisors. Borrowers who require support in completing their submission can avail of our 'assisted' option. Multiple user scenarios and workflows were considered to ensure we had an online SFS solution relevant and accessible irrespective of the borrower circumstance.

Since this initiative started the return rate on the online SFS is averaging c. 30% which is significantly higher than the email SFS c. 10% and the paper SFS c. 18%.

We hope that benefits will increase in line as we continue to drive digital adoption. A key next step is to enable customers already engaged with the bank, who have pre-existing credit solutions in place, to leverage the digital offering as those solutions expire or require an adjustment.

CLICK HERE TO VIEW THE VIDEOS

Simple, concise video tutorials to help guide customers.



SAVINGS OF:

- **C.15K** KG IN WOOD
- **C.42K** GALLONS OF WATER
- **C.34K** LTRS OF CARBON (CO_2)
- **C.2.4K** LBS OF WASTE

CYBER SECURITY AND BUSINESS SYSTEM RESILIENCE

OUR APPROACH

The cyber threat landscape continues to grow and evolve, encompassing existing and new technologies and exploiting vulnerable users. Cyber security incidents and the related costs make it a financially material issue. Ensuring the security and resilience of networks and information systems is critical.

Our Board is responsible for cyber strategy and the Risk & Capital pillar of our Group Strategy has a strong focus on IT Resilience. Within our Executive Committee, our Chief Technology Officer is responsible for cyber security. Roles and responsibilities in Information/cyber security are set out in our Information Security policy.

Recognising the strength of wider collective effort in the fight against cyber crime, we partner with other banks across Europe through the Banking & Payments Federation of Ireland and the Cyber Defence Alliance, playing a role in fostering an open, knowledge-based and mutual protection culture that enhances the ability of all participants to protect against cyber threats.

We seek out innovative ways to continue to deliver resilient systems. In 2020, we completed a two-year project to move 95% of AIB's data to modern high tech virtual disk storage, underpinning an increasingly digitised future. This provides great benefits to our business system resilience, enhancing our data recovery capabilities.

INFORMATION SECURITY STANDARDS

Our systems are designed and operated to remain secure, while providing products and service that are fit for purpose. AIB is accredited for ISO 20000 2018 standard certification for service management systems (which underpins our IT infrastructure). We have well-established, comprehensive Information Security Standards in place for in excess of 15 years. They are aligned to ISO 27001, reviewed regularly and subject to independent review by a third party annually. All our employees, contractors, consultants and third parties including those involved in sponsoring, developing, supporting, implementing, administering, operating or otherwise delivering IT solutions must understand and comply with them. Our Information Security Management System extends beyond our Standards. Our Board approved cyber strategy sets out our security purpose, principles and objectives. An overarching Information Security Governance forum is supported by a number of groups that ensure AIB's information and technology assets are secured and protected. Our Data Governance Committee provided oversight, direction and transparency in decision making, assists in maintaining good information security hygiene and provides an escalation plan to Board, where required.

CONTROLS

The threat landscape is constantly evolving and accelerating and our controls are monitored and tested regularly to prevent unauthorised parties from accessing, manipulating or acquiring data. We operate internal control testing aligned to the NIST Cybersecurity Framework. We have business continuity plans and incident response capabilities in place, and test them at least annually. And we drive the delivery of new and enhanced controls to ensure we keep pace. To assure the security of the IT systems and data we complete external verification and vulnerability analysis. External verification is delivered through external audits which are completed at least annually. Vulnerability analysis includes objective-based testing that simulates real-world cyber-attacks. 80% of our IT infrastructure is aligned with ISO 270001 and NIST. AIB continuously monitors key cyber risks and we understand what we must protect to keep AIB and our customers safe. AIB has a dedicated Security Incident team to analyse and respond to suspicious events. The team can be contacted by email, phone, on our Intranet or using the reporter button embedded into our email. Our Cyber Threat Intelligence team collate and evaluate intelligence on known and emerging cyber threats targeting financial institutions. In 2020, AIB did not experience any successful breaches of confidentiality as result of a cyber security incident, nor did we have incidents to our IT infrastructure which resulted in penalties or revenue losses.

CYBER RISK MANAGEMENT

Our Information Security, IT Risk and Continuity & Resilience policies support management of cyber risk in AIB. The Group's exposure to cyber risk is monitored by the Board through its regular risk reporting and focused updates on specific cyber-related topics. Our Chief Risk Officer's report for Group Risk Committee and Board Risk Committee on the risk profile of the Group and emerging risk themes. Cyber risk interacts with our Material Risks to varying degrees, and we see it as a sub-risk within our Operational Risk framework. Key cyber risk indicators monitored by the Board in 2020 include Investment in cyber security defences; and the number of high-impact cyber security incidents.

We operate our cyber defences in line with international standards, combining controls that help predict, prevent, detect and respond to attacks. We continue to improve our defences and control environment, which have proven robust to date. Nonetheless, the cyber threat profile remains elevated, with the threat landscape becoming more diverse, and attacks increasing in sophistication and volume.

AWARENESS & TRAINING

To ensure awarness of information security matters all employees are required to complete Information Security training which covers our policy, data protection law, reporting and escalation of issues. Additional training must be completed by high risk users. Training is underpinned by ongoing phishing simulations, the results allow us to measure AIB's resilience to such attacks. Typically we conduct one simulation exercise per quarter for all employees. However, in response to COVID-19, and to increase security awareness, we conducted additional simulation exercises in Q2 2020. In 2020 we completed eight phishing simulations in total – five for all employees and three directed at specific high risk users. In total we sent 70,734 phishing simulation emails in 2020 increasing from 63,624 in 2019. In 2020, our Board received cyber training from our Chief Information Officer and 96.5% of our employees completed our mandatory Information Security training.

CYBER SECURITY AND BUSINESS SYSTEM RESILIENCE

DISTRIBUTED DENIAL OF SERVICE PROTECTION (DDOS)

The DDoS replacement program supports our system resilience by ensuring that we have the appropriate defence mechanisms in place to prevent a sustained outage on our customer or employee channels.

As the risk of a malicious attempt to disrupt business through a DDoS attack has increased, we have looked to invest in a state-of-the-art solution to support our strategy. A DDoS attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable by temporarily or indefinitely disrupting services of a host connected to the internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. This typically manifests as a significant and sustained interruption of a company's web presence.

To protect against these attacks a dual vendor DDoS solution, one providing DDoS mitigation on- premises and one cloud based mitigation solution were successfully deployed in 2020.

This solution responded to a DDoS attempt in July and the solution successfully defended the attack. If successful, this attack would have caused a sustained customer outage on our online banking and mobile platform, and all employees working remotely would have been unable to connect to our network.

MIGRATION TO NEW DIGITAL PLATFORM FOR SMES

In 2020 we delivered a new digital banking platform for SMEs providing them with a richer, better user experience. The program is expected to reach completion in H1 2021.

- The new platform now supports over 90% of all our payment types offered and carries over 80% of our payment traffic. International payments in 28 currencies are also supported
- We have removed the complexity from making payments by guiding customers through the journey – making the job of paying invoices and employees easier whilst ensuring that payments reach their destination as quickly as possible
- We have extended the balance and transaction history service from two to four years, made it easier to search for historical transactions and added new eStatement capability for most bank accounts registered on internet Business Banking (iBB)
- A range of self-serve functionality has been added including the ability to confirm security credentials (removing the requirement to go to Branch for this service)
- We are now delivering Application Programming Interfaces (APIs) off the new platform for account and payments services for all customers. We are now also providing APIs for bulk and international payments. 89% of customers indicated they are able to fulfil the purpose of their logon
- The programme continues to add new functionality as part of the ongoing release schedule. An example of new functionality to be delivered in Q1 2021 is the ability to reverse sell and forward contract dealer rates.

PROTECT OUR CUSTOMERS' DATA AND PRIVACY

OUR APPROACH

Our customers trust us with their information, and we have a responsibility to keep this information safe and transparent in how we use and protect our customers data.

Our Code of Conduct sets out that AIB expects employees to maintain high standards of physical, information, and digital security. We respect all personal data that we process, and we have a responsibility to keep this information safe. Augmented processes and procedures we have set up to comply with the General Data Protection Regulation (GDPR) programme have helped us to build on our existing data protection capability and ensure we are fair and transparent in how we use and protect our customers data.

We require our employees to complete mandatory training on data protection. In 2020, 92% of employees completed our Data Protection training.

DATA PROTECTION OFFICERS

To support this we have a Data Protection Officer (DPO) in both Ireland and in the UK. Our DPOs set our Data Protection Policy and oversee its implementation across the organisation. In our Data Protection Notice we inform customers of their rights and how we process their data. Our DPOs are the point of contact for customers who have queries/complaints about how we process their data or personal data breaches. They also interact with the Data Protection Supervisory Authorities in Ireland and the UK. In 2020, the Irish DPO presented the DPO report to the Board Risk Committee. This report provides a summary of the key thematic areas and emerging risks and associated mitigating actions.

The Group Privacy Office is responsible for embedding data protection by design and default across our business and ensuring that privacy considerations are at the heart of the decisions that we make, ranging from developing new products and initiatives to the on boarding of new suppliers. Our Data Rights team support data subjects who exercise their data protection rights.

RISK MANAGEMENT

Management of data protection matters is covered by our Operational Risk Framework and our Data Protection Policy, and supported by a comprehensive suite of complimentary policies including our Data Risk Policy (which includes Ethical Data Handling risk).

Our Regulatory Compliance team is specifically responsible for independently identifying and providing an initial assessment of current and forward-looking compliance obligations including regulation on privacy and data protection. The Data Protection Policy is part of the Regulatory Compliance Risk Management Framework. It aims to ensure that processes and controls are in place to minimise the risk of unfair or unlawful data processing and all employees understand the responsibilities and obligations that must be adhered to under Data Protection regulation. It applies to our entire operations, including our suppliers. Any material changes to the policy must be approved by our Group Risk Committee.

REGULATORY DEVELOPMENTS IN 2020

Our DPO's team provides ongoing advice on Data Protection issues. Compliance monitor the regulatory horizon to ensure continued compliance. In 2020, COVID-19 presented heightened data protection risk, with an increase in the volume of special category data being held by AIB Group and the shift in employees working remotely. We have followed all relevant government and regulatory guidance on these matters and will continue to do so.

The European Court of Justice decision in the Schrems II case raised a number of matters about the transfer of personal data to countries outside of the EEA (including the UK post Brexit). The implications of this decision on all data transfers to third countries remains a key area of focus for AIB to ensure any such transfers are taking place in a lawful way.

In Ireland, the Data Protection Commission (DPC) published Guidance on Cookies and other Tracking Technology, and we have mobilised a project to ensure compliance with this in Q1 2021.

In the UK, the Information Commissioners Office (ICO) published guidance (covering topics including AI, data sharing and accountability) and its Age Appropriate Design Code – a Statutory Code of Practice which sets 15 standards and explains how GDPR will apply for children using digital services.

BREACHES OF PRIVACY & LOSSES OF DATA

In this disclosure we refer to complaints on GDPR. The majority of these relate to events in preceding years. In 2020, we received 23 complaints from the DPC and one from the ICO regarding breaches of data privacy. The majority of these related to alleged failures to comply with data subject access requests. 18 of these complaints were closed by the DPC and one by the ICO following engagement with AIB.

Following the judgement in the Schrems II case, the Bank received a complaint from 'None of Your Business' alleging that AIB continued to use Facebook Connect – a tool that collects data on people who visit our Facebook page and then sent it from the EU to the US for processing without any safeguards as Privacy Shield has been invalidated and there were no Standard Contractual Clauses in place. A response to the complaint was sent to the DPC and we are awaiting a response.

In 2020, we reported 132 personal data breaches under GDPR to the DPC and one to the ICO. While these may include losses of customer data or inaccuracy, the majority of those we reported related to unauthorised disclosure of personal data.

TO LEARN MORE CLICK HERE

To read our **Data Protection Notice** click here.

PROTECT OUR CUSTOMERS' DATA AND PRIVACY

DATA ETHICS & GOVERNANCE

As we continue to develop our technologies and advanced analytics platforms to deliver better customer experiences and relevant personalisation, we aim to do this responsibly.

Our Data & Analytics team have developed our Data Ethics Principles to guide our organisation on responsible data usage. These principles will ensure we continue to take an ethical approach on topics like data privacy, fairness, transparency and equity, by applying them to all our data activities in areas like AI and algorithmic design and data-driven technology development. A dedicated training module has been created to support the Data Ethics Principles. This module has been successfully piloted with the Data & Analytics team in advance of wider roll-out across the Bank.

To support our responsible data initiatives, we have piloted our approach to algorithmic fairness modelling and AI, with a wider roll-out planned for 2021.

Our Data Governance structure and control environment has been enhanced significantly, strengthening our risk data aggregation capabilities and reporting practices, to improve our risk reporting and data management. Focus areas for 2021 will be on key data remediation gaps, driving further adoption of data management tools and further enhancements to customer interactions, with some residual challenges from historical systems and processes to be addressed. We will continue to provide business insights and support to our leaders and enable a wide range of key programmes across the organisation.

DATA CENTRE MODERNISATION

In each of our Data Centre's, we held two tape silo enclosures which once housed approximately 95% of all the banks data. We recently completed a modernisation moving from tape data to virtual disk storage. We are the first bank in Ireland to do this and one of very few in Europe (as it is difficult to fully remove tape safely from a data perspective).

- 28,000 tapes have been professionally destroyed. The data has been moved on to modern virtual disk storage. This is important as tape is considered a weakness in terms of data recovery
- Our Data Centres have moved fully to Green Energy reducing power consumption by 30%, until recently our Data Centres consumed approximately 1/3 of the banks overall power
- Almost 100 large physical Unix servers that support some of our critical customer channels have been replaced with four smaller but more powerful and energy efficient servers, occupying 85% less data centre space.

CORPORATE GOVERNANCE AND ACCOUNTABILITY

OUR APPROACH

Our stakeholders tell us that corporate governance and accountability are important to them. Fostering a strong culture of accountability, integrity and openness, supported through appropriate governance and regulatory frameworks is a key tenet for our future sustainability. AIB's involvement with the impacts with the material topic corporate governance and accountability is cause and the key stakeholders are investors.

The Group's Governance Framework underpins effective decision-making and accountability. It is the basis on which the Group conducts its business and engages with customers and stakeholders. It ensures that organisational and control arrangements are appropriate to the governance of the Group's strategy and operations and the mitigation of related material risks.

AIB's corporate governance practices meet the many statutory and regulatory obligations that apply to the Group.

We have a diverse Board with strong knowledge and expertise, a robust governance structure and appropriate controls and oversight. Our Corporate Governance Structure is set out on p.15 and details of our Board of Directors are set out in our Annual Financial Report.

BOARD TRAINING & DEVELOPMENT

To support our Directors in their roles, we run a professional development and continuous education programme. In 2020, virtual training sessions covered topics included BCBS 239 Regulation, Internal Rating Based Models, Cyber Security Strategy, Resolution Planning, Safety & Wellbeing, Anti-Money Laundering and Fraud, Regulatory Accounting requirements, Directors Duties and the Market Abuse Regulations. Our Directors also have access to an online Corporate Governance Library and a suite of AIB specific online training courses.

BOARD DIVERSITY

The Board recognises that diversity and inclusion in its widest sense is important and is focused on ensuring a truly diverse board. The Board embraces the benefits of diversity among its members and through its succession planning is committed to achieving the most appropriate blend and balance of diversity possible over time.

In reviewing the Board composition, balance and appointments, the Nomination and Corporate Governance Committee considers candidates on merit against objective criteria and with due regard for the benefits of diversity, in order to maintain an appropriate range and balance of skills, experience and background on the Board and in consideration of the Group's future strategic plans.

At 31.12.2020 there was 56% female representation on our Board.

CLICK HERE TO READ MORE

Download our **Board Diversity Policy**.

CORPORATE GOVERNANCE AND ACCOUNTABILITY

CULTURE PROGRAMME

CULTURE EVOLUTION

Over the past year, there has been significant inroads and progress to the Culture journey in AIB. At the beginning of the year, with the help of ExCo and our Board, refreshed values and associated behaviours were created for the organisation.

Our values were launched in July with several initiatives to ensure employees understood, activated, and embedded the new values and behaviours into their teams. Over 2,200 employees engaged in the Culture journey awareness and People leader sessions. There was a keen sense of "tone from the top" as the top 100 People leaders in the organisation facilitated roundtable discussions with over 2,500 people, receiving valuable and honest feedback.

The next phase of the Culture journey is the commencement of leadership behaviours and mind-set changing. We know that leadership is a core component of culture and the shadow that leaders cast can have either a positive or negative impact on the culture. We want to ensure that all leaders cast a consistent positive shadow as leaders. To enable and facilitate that change, all leaders will participate in structured workshops which aim to 'unfreeze' current behaviours and habits by deepening participants understanding of our culture and underlying behavioural issues prevailing, and how the impact strategic delivery, business operations and employee engagement.

The ExCo and their senior management teams (circa top 100 leaders) participated in these workshops in Qtr. 4 2020. Our culture must be owned, and role modelled by senior leaders in the first instance – hence why we have started with senior leaders. Our remaining People Leaders will undergo a similar facilitated process in 2021 as part of a wider People Leaders Development Academy.

To ensure we are driving a Purpose led Culture, we evolved our Purpose Wheel to communicate our values and behaviours – with three core elements;

- **Why we do business** – to back our Customers to achieve their dreams and ambitions
- **What** – is our strategy under the five pillars
- **How** – we live our values and behaviours.

Our culture is the key enabler of our strategy and purpose and we are very proud of that. As we look at what best describes all elements of our culture – 'It's Who We Are' is the manifestation of everything we do – the products and services that we build and deliver for customers; how we support our communities and how we continue to support our colleagues across the organisation to grow learn and develop. Our culture is the sum of all the parts of these aspects of our work. As we continue our journey, we focused on the sustainment of Culture evolution.

OUR REFRESHED VALUES

- BE ONE TEAM
- OWN THE OUTCOME
- DRIVE PROGRESS
- SHOW RESPECT
- ELIMINATE COMPLEXITY

ETHICS AND INTEGRITY

OUR APPROACH

We rely on trust for our social licence to operate, and trust in banking is highly dependent on acting ethically and with integrity. It is no surprise that our stakeholders see ethics and integrity as a material topic. Our involvement with this material topic is cause, and the key impacted stakeholders are customers and society.

Our Code of Conduct is a core framework that underpins our values and culture. It sets out clear expectations for how we behave and how we do business. It is vital that everyone who works in or for AIB understand how they are expected to behave. Our core values, principles, standards and behaviours are contained in our Code of Conduct.

The Code has evolved over many years, providing a guiding framework for many of our people policies on behaviour and conduct. It is underpinned by policies including Conflicts of Interests, Anti-Bribery & Corruption, Conduct of Personal, Financial and Tax Affairs, Social Media, Diversity & Inclusion and Speak-Up. It is owned and managed by Human Resources, and is supported by our Conduct Risk Framework.

All employees are required to adhere to our Code of Conduct and are required to complete a declaration of compliance with our Code as part of the annual ASPIRE performance management process. Failure to comply with our Code is taken seriously and may lead to disciplinary action up to and including dismissal or in the case of contract staff or suppliers, cancellation of contract. Annual training on the Code, delivered through iLearn – our e-learning tool, is mandatory for all employees, and completion is recorded, monitored and tested by local business teams with central oversight from Human Resources. In 2020, 93.2% of our employees completed our Code of Conduct training.

GOVERNANCE AND OVERSIGHT

The Chief Executive Officer is the policy sponsor of the Code. It is reviewed annually by our Group Conduct Committee and the Board Audit Committee and approved by the Board. An annual Code of Conduct activities report is presented to the Board Audit Committee on:

- the previous year's activities
- developments for the Code and its associated policies
- awareness levels of the Code
- aspects for review
- breaches identified and actions taken.

ENHANCING OUR CODE

In 2020 we updated our code of conduct to make it more user friendly and accessible for all employees, and the updated code was formally launched in February 2021.

Our personal responsibilities to abide by the Code are explicitly called out as are the responsibilities expected of all People Leaders to support and embed it. Our updated Code of Conduct now contains five core conduct standards that are reflective of those set out by our regulators in the jurisdictions in which we operate. The updated Code contains a guiding framework to help staff to make better decisions.

In February 2021, we launched our Human Rights Statement. This statement, which pulls together all the Human Rights commitments across the Group, is designed to support our Code of Conduct.

RAISING CONCERNS

Every organisation faces the risk that something will go wrong either accidentally or otherwise. It is very important that we hear about such things, at an early stage, so we can fix them.

We have well-established processes in place in AIB for raising and handling concerns, through the three mechanisms:

1) whistle-blowing
2) grievance
3) complaints.

CLICK HERE TO READ MORE

Learn more by reading our **Code of Conduct**.

CLICK HERE TO READ MORE

Discover more about making a complaint.

CLICK HERE TO READ MORE

Learn more by reading our **Human Rights Commitment**.

ETHICS AND INTEGRITY

WHISTLE-BLOWING PROCESS

Our whistle-blowing process is called 'Speak Up'. Under Speak Up, concerns can be raised anonymously but this may limit our ability to fully investigate them. Our Grievance process is a mechanism for our employees who feel they have been mistreated or have been subject to behaviours they believe are contrary to our Code of Conduct. We operate a comprehensive complaints process designed to provide our customers with the opportunity to be heard, have concerns investigated and make good where needed. See p.77 for more information.

Our Speak Up policy provides guidance on reporting wrongdoing or suspected wrongdoing through a number of channels, without fear of or actual retaliation, including:

- reporting issues to local management
- a reporting line to a nominated member of senior management
- access to a confidential internal telephone line or a dedicated Speak Up "@aib" email address
- an external, confidential, telephone and email facility operated by an international specialist charity, Protect.

Through the Speak Up process, concerns were raised on the following in 2020:

- Personal grievances
- Workplace issues (such as non-compliance with internal policies, information security issues, operational issues, etc.)
- Business policy decisions arising from COVID-19 Health and Safety issues
- Suitability of products for specific groups of customers.

In 2020 all guidance requests and concerns raised were successfully concluded by dedicated case managers.

TRAINING & AWARENESS

It is important that all employees are aware of our Speak Up process. Annually they are required to complete mandatory online training on Speak Up. The training module notifies employees about Speak Up policies and processes as well as the contact details and channels for raising a concern. In 2020, 92% of employees completed this training. Training has also been provided to managers on how to handle concerns appropriately.

GOVERNANCE

The Chief People sponsors our Speak Up policy while an Executive Committee subgroup has responsibility for reviewing Speak Up cases and follow-up actions. Two Non-Executive directors are Speak Up champions for the UK and Ireland. Investigations are conducted, as appropriate, by Human Resources (HR), business representatives and/or a specialised team in Group Internal Audit (GIA). We may engage an external investigator if appropriate in the circumstances. In cases of suspected fraud, GIA undertakes the initial investigation, and regulatory and policing authorities are notified if necessary and appropriate.

2020 ENHANCEMENTS TO SPEAK UP

- A new Head of Speak Up was put in place and Speak Up champions were appointed at Board level for Group and the UK.
- A communications plan was developed with the Chief People Officer.
- HR ran focus groups on Speak Up, and 186 employees took part in them. Feedback included that examples of real life whistle-blowing should be discussed more openly, and employees wanted to understand issues raised and how they were dealt with.
- Under our new Responsible Supplier Code, we extended access to whistle-blowing to our suppliers.
- We developed a new external portal to allow employees convey concerns through a digital channel. It will be launched in 2021 and be available 24/7.
- In June we published our first Protected Disclosures report. It is publicly available along with our Speak Up Policy at **www.aib.ie/sustainability**.

We will continue to build on the awareness of Speak Up as an appropriate channel to escalate internal issues in a safe and confidential manner.

CLICK HERE TO READ MORE

Read our **Speak Up Policy**.

CLICK HERE TO READ MORE

Download AIB's **Protected Disclosures Report**.

ETHICS AND INTEGRITY

ANTI-BRIBERY AND CORRUPTION

The most significant corruption risks faced by the banking industry relate to money laundering and terrorist financing, corruption in the supply of goods and services to the bank, internal and external fraud, conflicts of interest in business transactions, market manipulation in share dealing, data protection breaches and theft.

To manage corruption and its associated risks, we have implemented two group policies – our Anti-Bribery & Corruption (ABC) policy covers what constitutes bribery and/or corruption and what is prohibited under the various regulations. Our Conflicts of Interests (CoI) policy governs both the giving and receiving of gifts, benefits and hospitality. It is reviewed annually. In 2020 it was refreshed to reinforce responsibilities in directorships, outside employments and business activities. These policies apply to all employees, contractors and suppliers operating within AIB. They are reviewed annually by stakeholders and material changes must be approved by our Group Conduct Committee.

In line with our Anti-Bribery & Corruption and Conflict of Interests' policies, all our operations across the group are assessed for risks related to corruption. No significant risks related to corruption were identified through the risk assessment during 2020.

CENTRAL REGISTER

Under our policy gifts, benefits or hospitality given or received, in excess of €50/£50/$65 (including cumulative gifts received or given to or from one donor) are subject to prior approval from the employees People Leader and must be recorded on a central register. Co-ordinators are appointed for each business area – they review the register monthly, ensuring it is in keeping with our policies, complete quarterly returns to the policy owner and report policy breaches or assurance issues.

All business areas are responsible for completing a monthly risk assessment of all registered activities to ensure they are in keeping with policy and identify those which might give rise to a potential or perceived conflict situations or corruption. Where additional management oversight is required, business areas must ensure local procedures are in place to mitigate bribery or corruption of any sort, and to ensure that employees are regularly apprised of the potential risks and mitigants required.

AWARENESS & TRAINING

Both policies are subject to annual stakeholder review and are supported by a mandatory e-learning. New employees and insourced suppliers (i.e. contractors and third-party service providers) are required to complete this training within one month of joining AIB and all employees are required to complete it annually. Roles and responsibilities documents and instruction guides are published on our intranet, to aid understanding of these policies.

Employees – An information mail on anti-bribery and corruption is issued at least once annually to all employees. In October we emailed all employees to notify them of the update to the CoI policy and remind them to complete their annual mandatory e-learning course, which also includes anti-bribery & corruption matters. In 2020, 91.5% of employees completed the training (91% Ireland, 96% UK and 94% USA). As subject matter experts, HR provide additional training and support to employees who oversee the central register and co-ordinate quarterly returns for their business.

Board – The Board Audit Committee oversees compliance with the Group Code of Conduct and Conflicts of Interests Policy by way of an annual update from Management. It also ensure that arrangements are in place for the proportionate and independent investigation of matters raised under that policy for appropriate follow-up action. Material matters relating to anti-bribery and corruption will be escalated to the Board by management on a case by case basis through Executive Management Reporting.

Suppliers – Our Responsible Supplier Code clearly sets out our expectations for our suppliers on anti-bribery & corruption matters. Our People Leaders are required to brief their insourced suppliers on it and our business owners brief our outsourced suppliers in accordance with our Third-Party Management (TPM) process. Additionally, guidance is provided to our suppliers through the TPM process. The level of training and support provided to suppliers depends on their risk rating.

RESPONSIBLE ENGAGEMENT

Our approach to lobbying is covered in our Conflicts of Interests policy, Anti-Bribery & Corruption policy and our internal Lobbying policy. In Ireland, AIB is registered as a lobbyist albeit we do not actively lobby. Lobbying activity in Ireland is recorded on the lobbying register. Political donations are prohibited under our Conflicts of Interests policy.

CLICK HERE TO READ MORE

View our **Conflicts of Interests Policy**.

CLICK HERE TO READ MORE

Read our **Anti-Bribery & Corruption Policy**.

CLICK HERE TO READ MORE

Find out more about AIB's lobbying activity in Ireland.

ETHICS AND INTEGRITY

OUR SUPPLIERS

We maintain a database of approximately 4,000 suppliers, with whom we contract. Our suppliers are based predominantly in Ireland and the UK however, we have a small number of suppliers based outside of this jurisdiction, mostly in the USA and India. Our principal spending categories are professional services, business services and information technology.

We segment our supplier base into five tiers based on risk and criticality of the service being provided; we manage these suppliers proportionately to the level of criticality or risk involved, thereby our most critical services in the highest tier (Tier 1) are the most closely managed, while the lowest tier (Tier 5) suppliers typically provide low value transactional type goods and services.

Market intelligence together with specific selection criteria and best-in-class supplier selection tools help us to select the most appropriate suppliers for the services we require.

We complete due diligence for supplier selection, prioritised according to the nature, value, complexity, and criticality of the service being procured. For high value/risk services, specific diligence checks are performed on the supplier and the proposed service model. Lower value/risk suppliers are subject to routine company financial and sanction scanning checks.

AIB suppliers must adhere to all legal obligations in each jurisdiction in which they operate or provide services (e.g., environmental and labour law), as well as any specific requirements included in AIB's own policies. Key suppliers must attest annually to key policies (or clauses in them that are relevant to our supply chain). These include our Code of Conduct, Conflicts of Interests policy, Anti-Bribery and Corruption policy and Data Protection policy. We also require that, where relevant, key suppliers conform to the UK Modern Slavery Act.

In 2020, we launched our Responsible Supplier Code that sets out our expectations of suppliers, and includes responsible and ethical behaviours we look for in the companies with whom we do business.

CHANGES TO OUR SUPPLY CHAIN IN 2020

During 2020, based both on our ambition to better manage third party risk, and adhere to European Banking Authority Guidelines on Outsourcing, we continued to reclassify our third-party arrangements (including Intra-Group and Financial Market Instruments relationships for example). As a result, we reclassified our supply base in terms of business risk, by virtue of the potential impact to AIB should the third-party service delivery be impacted or fail, taking into consideration their products and services, business continuity measures, human resources, anti-bribery measures, environmental and their approach to responsible business.

OUR RESPONSIBLE SUPPLIER CODE

In October 2020 we published our first Responsible Supplier Code to our supplier facing website. The code sets out the minimum standards we expect of our suppliers. The term 'Supplier' as used in the code refers to suppliers, vendors, contractors, consultants, agents and other providers of goods and services who do or seek to do business with AIB Group.

In Section 1, we outline our approach to responsible and sustainable business setting our expectations for suppliers, and the key social, ethical, and environmental values to abide by. We want to support an inclusive ethical supply chain and ensure that individuals and companies throughout our supply chain work responsibly, sustainably, and safely. This Code is based on our Code of Conduct which incorporates these commitments, our values and responsible business approach to support the delivery of our business objectives.

In addition to the Code of Conduct, the Responsible Supplier Code references some of our policies which are intrinsically linked with ethical and responsible behaviour such as: Anti-Bribery and Corruption policy; Conflicts of Interests policy; Modern Slavery Statement; and our Speak-Up policy.

The Speak-Up policy informs the supplier of how to raise a concern should something go wrong or if they suspect a wrongdoing.

In Section 2, we set the minimum expectations we have of our suppliers in relation to Human Rights, Health safety and Welfare, Supply Chain, Diversity & Inclusion, Doing Business Responsibly and Sustainably.

The last section of the code details our commitment, and how we will support the supplier to align to our values and principles.

We expect our suppliers to conduct business in a fair and honest manner with all their stakeholders, employees, subcontractors and any other third parties. AIB will only engage with suppliers who adhere to our Responsible Supplier Code. We require our suppliers to evidence that they have an Environmental, Sustainability, and Governance (ESG) plan in place, or are working towards putting one in place. All successful suppliers are required to join the Supplier Financial Qualification System (FSQS). AIB commits to being carbon neutral by 2030, and we will require the support of our supply chain and their suppliers to help us achieve this.

CLICK HERE TO READ MORE

Learn more by reading our **Responsible Supplier Code**.

COMPLY WITH LAWS, CODES AND REGULATIONS

OUR APPROACH

Compliance with laws, codes and regulations helps our stakeholders to trust us. AIB's involvement with this material topic is cause and the key impacted stakeholders are customers and investors.

REGULATORY COMPLIANCE

We have a strong approach to regulatory compliance in AIB, with management responsibility for it aligned with our Three Lines of Defence (3LOD) approach to risk management. Our Regulatory Compliance Risk Management Framework, approved by Board Risk Committee, sets out the principles, roles and responsibilities, internal controls, and governance in place to achieve compliance objectives. It is underpinned by policies designed to protect our customers, such as Data Protection (p.73) and Financial Crime.

In 2020, we self-identified two incidences of non-compliance which we notified to the relevant regulators. The first related to the Competition & Markets Authority's Bundling Undertakings on SME Lending, which has been addressed and closed. The second related to not being fully compliant with the Data Protection Commissioner's Guidance Note on Cookies and other tracking technologies in 2020. A project has been mobilised to ensure compliance in Q1 2021. Neither incidence was systemic and neither resulted in a fine/non-monetary sanction.

FINANCIAL CRIME

Financial Crime is managed through our 3LOD approach. Our Money Laundering Reporting Officer (MLRO) is responsible for oversight of our Board's compliance with AML law, which is externally supervised by the Central Bank of Ireland, the Financial Conduct Authority (UK) and the Department of Financial Services and Federal Reserve Board (USA). Our robust Financial Crime Framework includes our Financial Crime policy and standards on Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT), Fraud and Group Sanctions. The policy and standards are embedded within our operating procedures, and subject to an annual content verification to ensure they are kept up to date.

All employees and Directors are made aware of our Financial Crime policy and standards. Employees must complete mandatory e-learning annually. Our MLRO (or Deputy) provides comprehensive annual training to the Board. Bespoke training tailored to consider the ML/TF risks relevant to the specific roles, is also provided. To further enhance awareness, Financial Crime AML and Sanctions Bulletins are issued periodically to our employees outlining key trends and other topical items.

Our customers go through our Customer Due Diligence process at the on-boarding stage and on an ongoing basis, which is driven by the risk category of the customer. Within the due diligence process, we screen customers against various criteria including national/international sanctions or terrorism. Some customers and beneficial owners present higher risk (for example, politically exposed person (PEPS) and/or customers established/ residing in a 'high-risk third country'). For them we apply enhanced customer due diligence. We have a two-tier escalated sign-offs for PEPs, with higher risk PEPs requiring approval by the MLRO. Our processes monitor the activity of our customers' bank accounts and transactions to ensure unusual activity is investigated and corrective action taken, including reporting any suspicious transactions. Our Financial Crime Risk team perform ongoing monitoring of all activities. We retain records on Business risk assessment, customer identification and transactions for seven years.

1,024
EMPLOYEES
REGISTERED FOR THE RISK SYMPOSIUM AND FOLLOW-UP EVENT

1,374
EMPLOYEES ATTENDING
30 TRAINING SESSIONS THROUGHOUT THE WEEK

RISK CULTURE

A key aspect of building a strong culture is have the right risk culture. It underpins effective risk management and sound risk taking. We define it as the values, behaviours, beliefs, knowledge, attitudes and understanding of risk shared by individuals and teams in our business.

Our risk culture is supported by our risk management methodologies and structures which are aligned to the Three Lines of Defence (3LOD) model – the First Line (business) owns and manages the risk, the Second Line (Risk) sets the frameworks and policies for managing risk and the Three Line (Audit) provide independent assurance of the risk management activities of the First and Second line. To help to enhance understanding of risk, all our employees are required to complete risk e-learning.

RISK AWARENESS WEEK 2020

We ran a Risk Awareness Week which featured with extensive input from senior leaders and attendance by over 1,000 employees was recorded over the week. Highlights included:

- An opening Risk Symposium where our CEO & CRO were joined by external speakers to discuss topical risk management issues such as COVID-19, Brexit and consumer advocacy and risk
- Panel discussions with ExCo members on what risk culture means to them
- Virtually delivered training sessions, covering topics including fundamentals of risk management, regulatory engagement, the upstream regulatory agenda, and individual risk management issues such as fraud, information security, credit, conduct and operational risk
- 'How to' videos posted internally featured employees from across the business talking about what the values mean to them in supporting risk culture, and stories of how teams across all three lines of defence demonstrated the desired values and behaviours to reduce risk and drive better customer outcomes.

COMPLY WITH LAWS, CODES AND REGULATIONS

THE RIGHT TO DISCONNECT

In 2020, COVID-19 brought about many changes in how we work. Over a weekend in March, employees with relatively basic equipment managed to keep business activity moving all over Ireland, the UK, and the US all from their own homes. While these efforts to keep a critical national service operational, it also shone a light on the efforts and hours spent by employees juggling multiple competing demands of work, school, and home life.

Recognising the need to support a heathier work life balance, we considered ways we could support our employees while they were trying like many to juggle work at home and personal responsibilities.

The result of this was an idea that became Work/Life Balance Guiding Principles issued in June and which were positively referenced by the Financial Services Union (FSU) as an example to other employers when talking about their Right to Disconnect Policy. On Morning Ireland on RTE Radio 1 in July, the FSU spoke about this joint initiative as a very progressive move, where AIB were first movers ahead of the publication of a statutory Code of Practice. The principles were fair and balanced to avoid an 'always-on' culture while setting out ways to manage that.

The guiding principles are as follows:

MEETINGS

- Schedule all meetings during normal working hours
- Avoid scheduling meetings during lunch time
- Respect people's time by only inviting them to meetings where they need to play an active role
- Block out time on your schedule where you are not available for meetings so that you can temper how much virtual communication you have each day.

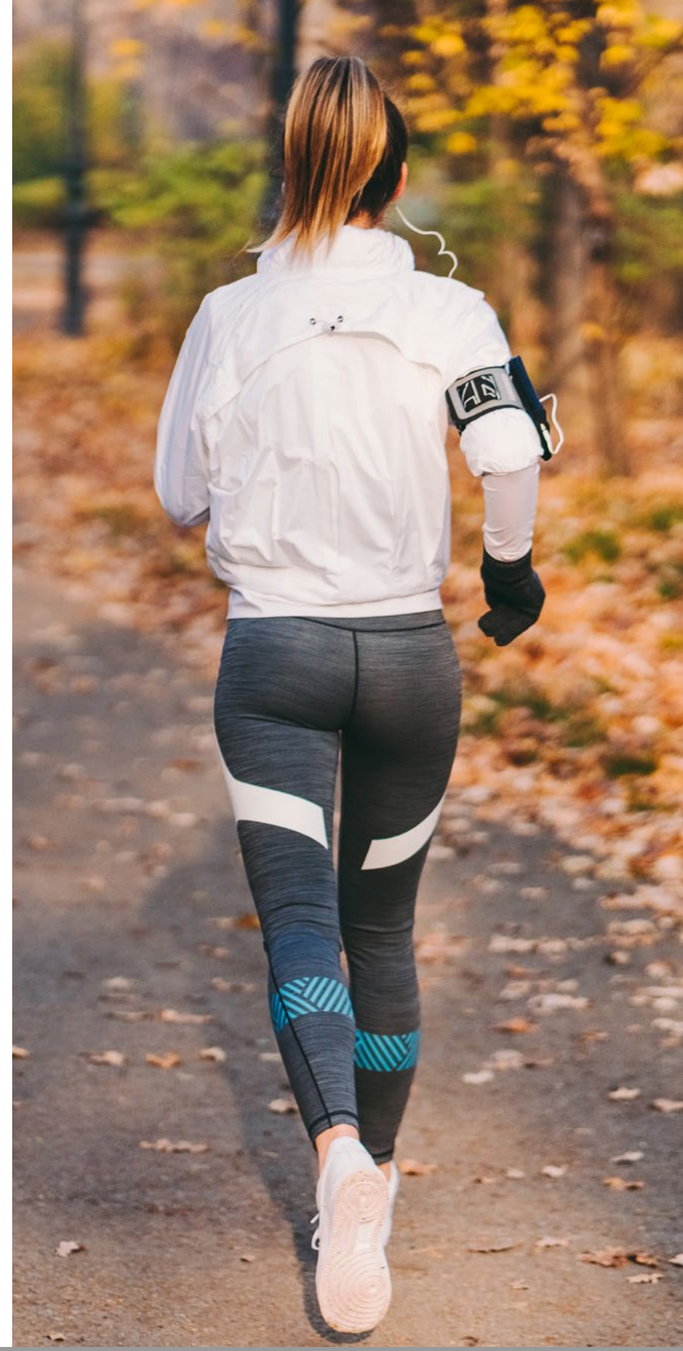
EMAILS

- Downtime is important, and we expect you to disconnect from work email on evenings, weekends, and during Annual Leave. Try to only check or send emails during normal working hours
- If it suits you better to send mails outside working hours either:
  - send the mail with a signature disclaimer at the end of it along the lines "I am currently working flexibly – so whilst it suits me to send this email now, I do not expect a response or action outside your own working hours"; or
  - use the "delay send" options and set it to a specified time the next morning (if it is a weekday)
- Employees might also consider putting their Out of Office on when they finish work and adding the following to their email signature: "My normal working hours are from x to y. I will respond to you when I am back in the office"
- In the case of an urgent or time-sensitive situation after normal working hours, please send a text or make a phone call
- On a social aspect, why not try adding some personal information to your email signature e.g., Joe Bloggs; Professional: Group Wellbeing Officer; Personal: Proud Limerick-man with a passion for sports.

OTHER GUIDELINES

- Schedule 2 hours of the day, to work on important things that require your focus and undivided attention, with your email and internet turned off
- Schedule and make sure you take your coffee breaks and lunch break.

Senior leadership fully endorsed these principles, and it was acknowledged that they do not expect an 'always-on' response from staff. It also brought important clarity on the importance on being able to distinguish leisure, family and working time for all employees.



TALENT ATTRACTION AND RETENTION

OUR APPROACH

In both delivering for our customers and investors today and into the future, attracting and retaining the best talent is critical to success.

EMPLOYEE SUPPORT DURING COVID-19

In March, in a short timeframe we enabled over 80% of our employees to work remotely. Those who worked in branches and contact centres had to adapt to new procedures that integrated a much more rigourous health & safety protocol into how they worked, to protect their own health, the health of their colleagues and the health of our customers. Our employees worked to keep 99.5% of our branches open, a real feat considering the situation society faced. For information on health and safety changes to our workplace see 'Banking safely during COVID-19' on p.47.

Our Chief People Officer and Chief Executive Officer regularly engaged with our employees throughout the pandemic. And our COVID-19 Hub on our intranet provided employees with easy access to all the information they need to support them through the pandemic – whether working remotely or onsite.

Safe working is an integral part of our culture, and COVID-19 has taken the importance of safe working to another level. Our Health & Safety policy forms part of our Safety Statement. It sets out the practical steps each of us must take to ensure the safety of our employees, customers, contractors, visitors, and our workplaces, and defines and communicates the roles and responsibilities for health and safety throughout AIB. It is supported by health & safety training and regular accident awareness communications. We report annually to the Board on health & safety activities.

We ran surveys in April, July, and November to measure how employees were feeling in the evolving situation, and to gauge if they felt they were getting the support they needed.

The April results showed us that employees strongly felt that their "People Leaders kept them informed about what was going on in AIB" and a significant percentage of the respondents also felt that "AIB has followed a clear plan of action in response to COVID-19".

In July, more than 80% of those who completed the survey felt:

- "AIB was concerned about employee health and wellbeing"
- "AIB was supporting employees to adapt to new ways of working"
- "AIB has communicated clearly and consistently during COVID-19".

November's results shows us that 85% continue to feel AIB is concerned for their wellbeing, and 87% feel communication was strong during COVID-19.

WELLBEING

Our wellbeing program launched in January 2020. It is pro-active and holistic in nature, and focuses on four key pillars – physical, mental, social, and financial wellbeing. Our four wellbeing channels are our advocate community, our intranet site, the Sports & Social Committee and our PepTalk app which has over 3,500 users.

Q1 efforts focused on physical wellbeing and were dedicated to exercise, sleep, and nutrition. They were supplemented by physical get active classes, and expert talks on sleep, exercise, and nutrition. We rapidly ramped up our program to provide continued and extended support throughout the pandemic.

The mental health pillar is employee-led, using internal talent with external expertise when required. We work alongside See Change to break down stigma around mental health. Recognising that poor financial health can be a key stressor, we recorded six financial wellbeing podcasts, facilitated by one of our Senior Economists and our Head of Customer Financial Planning, to give employees the low down on a range of financial matters. When our employees have issues that affect their work or home life, they have the option to use our Employee Assistance programme – an independent and confidential work-based support service that is available free to all employees.

The programme gained significant traction amongst employees' and key to its success is our 'wellbeing for staff by staff' approach. We have 120 advocates who promote the programme and they keep their teams up to date and have organised on average 305 wellbeing activities per month.

DIVERSITY & INCLUSION

We commit to creating an inclusive and supportive organisation that delivers a superior experience for all our customers, providing an extraordinary place to work for our employees, and offering an appropriate financial return for our shareholders and the economies within which we operate. Our Diversity & Inclusion Code operates as part of a suite of standards that support our Code of Conduct. The Diversity & Inclusion Code is available on our website **www.aib.ie/sustainability**.

At year end we had 56% female representation on both our Board and Executive Committee. More details on female representation and our age profile is set out on p.99. Family leave options to support working families help to support our diversity agenda, and in 2020 we made available enhanced maternity, paternity and parental leave options for all employees. Recognising that in order to achieve our wider gender balance agenda, we have invested and supported programmes to encourage and support females in primary, secondary and third level institutions.

We have six employee-led resource groups, covering Family, Women, Men, Roots, Ability and Pride matters helping us to create a sense of inclusion for all. Some of the many events marked virtually in 2020 included Pride Month, Diwali and Black History Month. The Women Matters group also coordinate successful peer-to-peer mentoring across the business.

CLICK HERE TO READ MORE

Download our **Diversity & Inclusion Code**.

TALENT ATTRACTION AND RETENTION

OUR APPROACH

GRADUATE PROGRAMME

Our graduates are an asset to the teams and business areas that they join – they bring new perspectives, fresh thinking, and great enthusiasm. In 2020, many of our graduates were chosen to work with the Sustainability Office to support the launch of Sustainable Communities as a pillar to our group strategy. The graduates shared their insights, energy and creativity and the experience gave them the opportunity to engage with senior leaders and stakeholders across the bank.

Over the last number of years, we have evolved our Graduate programmes to become 'best in class'. Winning the gradireland award in 2020 for 'Most popular graduate recruiter in Banking, Investment and Financial Services' award was a great endorsement of our programme.

EMPLOYEE TRAINING AND DEVELOPMENT

Employee training and development is critical in attracting and retaining the best talent. Our employees can access a wide range of training options and employee development and leadership development programmes. Due to COVID-19, face-to-face training could no longer be delivered and new ways of delivering training were quickly mobilised. We converted over 20 classroom-based courses into Virtual Instructor Led Training, both soft skill and technical courses, allowing for upskilling of new and existing employees. We created a new suite of support guides for People Leaders and employees, to help them to led through and work through remote working. Each guide contains practical frameworks, tips, tools and aligned learning resources. We continued to run our leadership programme creating a series of webinars and virtual training sessions.

We require our employees to complete a series of mandatory training annually. In 2020, our courses and completion rates were:

- Speak Up (92%)
- Anti-Money Laundering & Terrorist Financing (90.4%)
- Information Security (96.5%)
- Data Protection (92%)
- Health & Safety (89%)
- Code of Conduct (93.2%)
- Conflicts of Interests (91.5%).

Our target completion rate for each course is 90%, (allowing for employees on who may be on leave). Those on leave are required to complete the training on their return to work. Where completion rates have not met our target, people leaders intervene.

Annually we run a Career Development week which showcases to our employees all of the career supports in place. This took place virtually in November and over 5,000 employees participated in 120 live events which covered a myriad of topics including Remote Working, Resilience, Motivating teams and Women in Leadership.

Employees are encouraged to complete Continuous Professional Development (CPD), and those in customer-facing roles, involved in the distribution of products must have and maintain relevant qualifications to comply with Minimum Competency Code requirements specific to the products they distribute.

THE INSTITUTE OF BANKING

In 2020, 6,945 AIB employees were listed as members of the Institute of Banking and 6,170 participated in the CPD scheme, completing a total of 66,795 CPD hours. 857 employees received a university award through the IoB for their studies and 18 executives have been awarded the Certified Bank Director designation.

PEOPLE & CULTURE RISK

The risk to achieving the Bank's strategic objectives as a result of an inability to recruit, retain or develop resources, or as a result of behaviours associated with low levels of employee engagement is known as People & Culture Risk. It includes the risk that the business, financial condition and prospects of the Bank are materially adversely affected as a result of inadvertent or intentional behaviours/actions taken or not taken by employees that are contrary to our overall strategy, culture, and values. Key codes such as our Code of Conduct and associated policies help us to manage this risk and our Group Conduct Committee monitors the effectiveness of our approach, the outputs through several mechanisms including our annual performance review process 'Aspire' and our employee engagement performance.

REFLECTING ON 2020

At the end of 2020, we had 9,095 employees across Ireland, the UK, and the US with 89% of our employees working in our Irish operations. 75% of our employees are covered by collective bargaining. In 2020, our employee turnover rate was 8.6%. By 2023, we expect to employ 1,500 fewer people due to a combination of normal retirements, natural exits, and Voluntary Severance.

Without a doubt, COVID-19 brought challenges for how we could continue to support our employees at this very difficult and unusual time. Despite this, as demonstrated in the outputs of our ongoing surveys, in 2020 our employees felt that their wellbeing is important to AIB, and they felt safe in doing their jobs. Our Wellbeing progamme provided support throughout the year and while we had to pivot our approach to training our employees, they were still were able to complete training – averaging at 24 hours/three days each.

LOOKING FORWARD

We have a steadfast focus on providing our customers with the best banking experience regardless of when or how they need us, strong customer advocacy is a key tenet of a sustainable business. This requires ongoing investment in our platforms, relevant training of our people, enhancements in our customer journeys and importantly learning from mistakes when things go wrong. We have included relevant targets to use as key indicators of our performance.

While embracing the opportunities the digital agenda represents for AIB, our controls, training, reporting and, where needed, remediation approach helps to prevent significant breaches or misuse of our customer data. The data agenda continues to advance, and as new technologies and approaches evolve, we expect it will continue to change and become increasingly complex and challenging.

You can find commentary on the key metrics we monitor in this chapter as follows:

- Net Promoter Scores (NPS) (see p.65)
- Digitally active customers (see p.46)
- Diversity – female representation (see p.83).

In 2021, we intend to continue to have a keen focus on supporting our employees and customers through COVID-19, as it continues to impact society. We also intend to expand our graduate programme further, offering graduates an opportunity to join an enterprise-wide rotational programme. In support of our Speak Up programme, it is planned to develop and share case studies of previous whistle-blowing, to build awareness. Also, our new Speak Up external portal will be launched in 2021. The concerns raised will be provided to us for investigation. The new portal will allow us to engage with employees who wish to remain anonymous.

The Risk & Capital pillar of our Group Strategy has a strong focus on our IT Resilience capability, and we intend to continue to invest annually across our technology infrastructure. This investment, supported by robust governance and a strong risk culture, will ensure our technology continues to be responsible and reliable and will enable us to continue to respond to the ongoing challenges.

We pledge to **DO MORE.**
AIB Sustainability

OUR TARGETS

2023
TRANSACTIONAL NPS [1]
53+

2023
>2.25M
DIGITALLY ACTIVE CUSTOMERS

ONGOING
GENDER BALANCED
BOARD & EXCO

[1] Transactional Net Promoter Score (NPS) is an aggregation of 20 Homes, Personal, SME, Digital, Retail, Direct and Day-to-Day Banking journeys.