

## Championing human and digital rights

# Investing... in a safer digital future

We work to support and respect human rights – both on and offline – for everyone affected by our business.

“

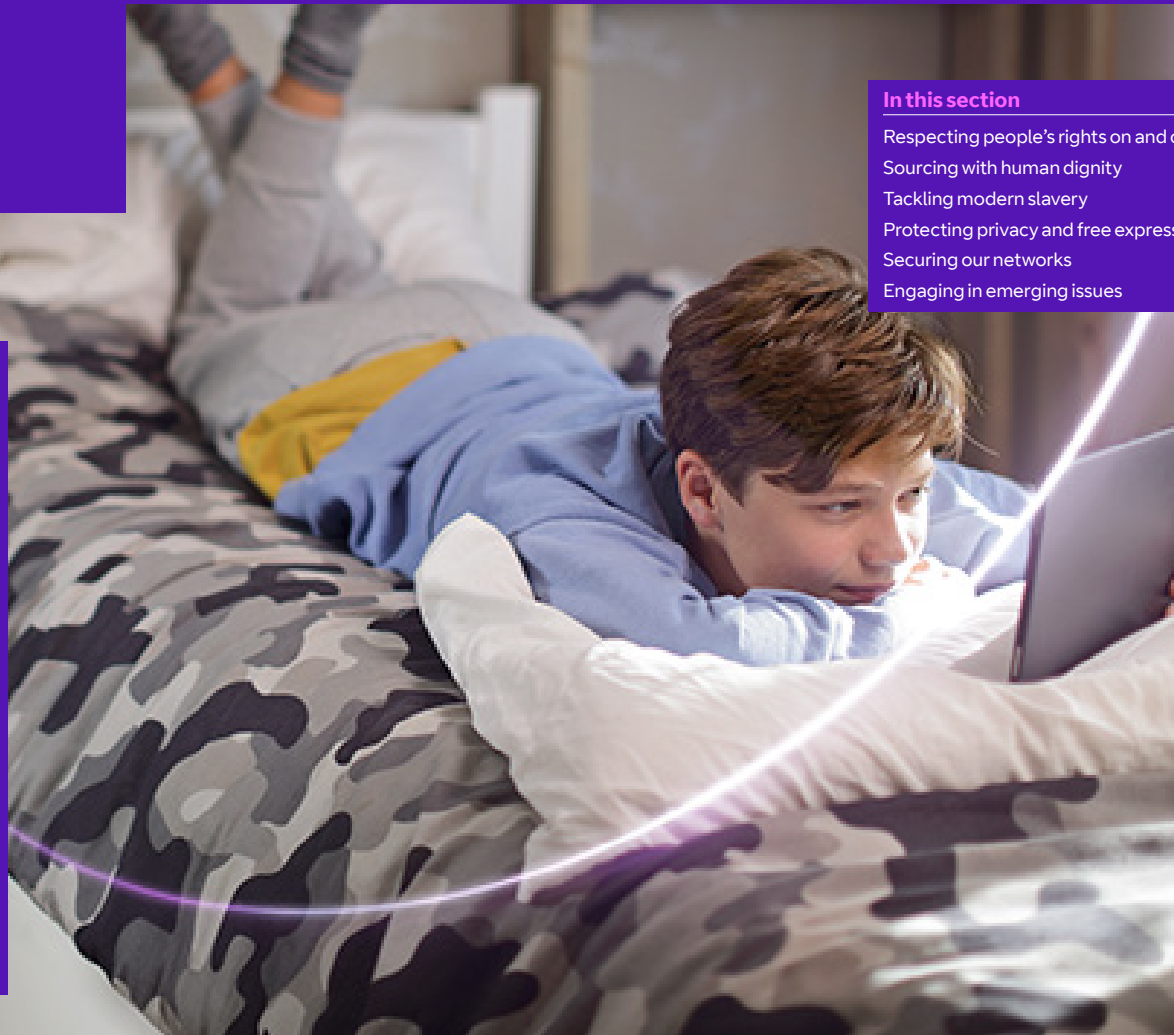
Respecting the human rights of everyone who comes into contact with our business is one of our most basic responsibilities. We pay close attention to identifying and managing human rights risks, both on and offline. We also look beyond our own business to our supply chain and how our products and services might be used, and use our influence to contribute to wider positive change.



**Ed Petter**  
Corporate affairs director  
(executive human rights sponsor)

### In this section

Respecting people's rights on and offline	16
Sourcing with human dignity	16
Tackling modern slavery	17
Protecting privacy and free expression	18
Securing our networks	19
Engaging in emerging issues	19



## Championing human and digital rights continued

### Respecting people's rights on and offline

Everyone is entitled to basic human rights and freedoms. We work to support and respect the rights of our colleagues, supply chain workers, customers, the communities where we operate and anyone else affected by our business.

Our products and services help people enjoy their rights and freedoms by accessing information and education, communicating with their families and staying safe online. But the digital age also brings new challenges to human rights, including threats to privacy and free expression, and the potential for misuse of digital technology. Complex global supply chains also carry risks to human rights.

We don't back away from these challenges. We adopt a principled approach in our business and supply chain. We engage in the debate on complex human rights issues and we work with others to harness the power of technology to contribute to positive change.

#### Respecting human rights in our own business and beyond

We're committed to respecting human rights in our business and through our broader relationships. BT was an early signatory of the UN Global Compact and we follow the UN Guiding Principles on Business and Human Rights.

Our [human rights policy](#) sets out our approach to human rights. It's supported by the [BT ethics code](#) that guides all our colleagues to recognise and respect the dignity and equality of everyone we work with.

Our people complete mandatory annual training on human rights as part of their training on the ethics code (see [page 33](#)).

This year, we asked the teams most likely to come across human rights issues – including colleagues involved in legal affairs, procurement and security – to complete a new additional online training module on human rights. The course helps them understand how to deal with potential real-life scenarios that could affect human rights.

We have due diligence processes in place for high-risk sales that have enabled us to identify the potential human rights impacts of a number of transactions this year. Where necessary, we followed up by conducting enhanced human rights impact assessments and taking specific actions to mitigate risks.

This year, we've expanded our dedicated human rights team to four experts, including one focused on privacy and free expression. We also raised Board awareness of emerging human rights issues for the tech sector through an expert briefing session for our *Digital Impact & Sustainability Committee*, which [oversees](#) our human rights programme.

If anyone has concerns, we want to hear them. We encourage our colleagues, contractors or suppliers to contact our human rights team or our confidential Speak Up helpline (see [page 33](#)) to raise concerns. BT colleagues can also use our internal 'Ask a Question' portal.

#### Championing human and digital rights

We advocate to accelerate change for the better across our sector and beyond. Our chief executive Philip Jansen signed the World Business Council for Sustainable Development [CEO call to action](#) to urge business leadership on human rights.

We take part in the debate to shape the conversation on human and digital rights issues – from modern slavery and privacy to emerging issues raised by technologies such as artificial intelligence (see [page 19](#)). This year, we gave input to the draft UN Business and Human Rights Treaty and the UN Human Rights in Technology Project ([B-Tech](#)). We're also continuing to sponsor [RightsCon](#), the world's leading summit on human rights in the digital age.



### Sourcing with human dignity

More than 14,000 direct suppliers in nearly 100 countries provide products and services to support our business – to the tune of around £13.8bn this year.

We expect our suppliers to share our commitment to respecting human rights. To sell to us, they must commit to our [Sourcing With Human Dignity](#) labour standards or equivalent, as well as our standards on climate change, environment, ethics, health and safety, and product stewardship.

Our pre-qualification questionnaire helps us decide whether or not to work with a new supplier by flagging potential risks, including those related to modern slavery (see [page 17](#)). We also use a risk-based approach that includes further research to check that our existing suppliers – and their suppliers – meet our standards.

This year, we identified 95 high and medium-risk suppliers that we needed more information from to better understand the risks and assess whether to take further action. In 53 cases, we undertook on-site assessments and we track progress on any issues identified to check improvements are being made.

If our assessments reveal any issues with compliance against our standards, we work with the suppliers in question to help them understand how to put the right systems in place and improve their performance (see box on [next page](#)).

## Championing human and digital rights continued

If a supplier doesn't show any commitment to improve, we may stop working with them.

We expect our suppliers to share our commitment to respecting human rights. To sell to us, they must commit to our sourcing with human dignity labour standards or equivalent, as well as our standards on climate change, environment, ethics, health and safety, and product stewardship.

### Looking deeper into our supply chain

We assess and follow up with all the high-risk suppliers that we purchase directly from. That's Tier 1 of our supply chain. But we're also checking standards further down the chain among suppliers that are less visible to us. This year, we've audited more of our suppliers' suppliers (our Tier 2) and some Tier 3 suppliers that were identified as high risk.

For one of our products, a cordless phone made in China, we followed the chain to assess suppliers at each tier down to the Tier 4 supplier that makes the plastic granules used to make the moulding that goes into one of the components of the phone itself. We also looked deeper into the supply chain of suppliers that provide services to us, such as engineering and call centre services.

We are members of the Responsible Business Alliance (RBA), who provide us with access to in-depth assessments of shared suppliers. We worked with the RBA to launch a new e-learning tool to help suppliers recognise and address the risks of modern slavery.

### Supplier assessments on social and environmental criteria

		2018/19	2019/20
Self-assessments by new or renewed contract suppliers		782	340 <sup>1</sup>
Suppliers identified as high or medium risk		368	95 <sup>1</sup>
% of high or medium risk suppliers reviewed within three months as follow-up		100%	100% <sup>1</sup>
On-site assessments (Tier 1, 2 and 3 suppliers)	Tier 1	40	15
	Tier 2	13	33
	Tier 3	0	5
	Total	53	53

<sup>1</sup> Numbers now only relate to contracted suppliers.

#### Case study:

### Working with suppliers to improve

We uncovered some issues during an audit of one of our SIM card suppliers that subcontracts its manufacturing to a company in Taiwan.

We assessed both companies – our direct (Tier 1) supplier and the subcontractor – and found several areas where they weren't meeting our standards. Some workers were being fined for sub-standard work, migrant workers in Taiwan had been charged recruitment fees, and we spotted health and safety issues too. We spoke to the suppliers to explain what we'd found and demanded urgent action to remedy the issues.

The Tier 1 supplier has since produced a development plan to rectify the issues and hired a dedicated manager to make sure it's implemented. Workers are already seeing improvements. Recruitment fees have been reimbursed to migrant workers and the other issues have also been resolved as the suppliers enhanced their focus on areas such as health and safety.

### Checking for conflict minerals

Electronic devices often contain small amounts of tantalum, tin, tungsten and gold. If these materials come from mines in conflict regions, there's a risk they could be funding armed groups or contributing to human rights abuses.

We work with suppliers to help prevent such conflict minerals being used in our products. Our [conflict minerals policy](#) sets out how. Each year, we report progress based on supplier assessments in our annual regulatory disclosure. And we keep track of best practices through the [Responsible Minerals Initiative \(RMI\)](#).

Cobalt, another mineral used in electronics, has recently been in the spotlight because of potential issues with working conditions and child labour. We're adding requirements on cobalt to our conflict minerals policy and due diligence process, using the [RMI template](#).

### Our responsibility to suppliers

Our relationship with suppliers is not one-way. We have responsibilities to them too. We're mindful that smaller companies in particular may rely on regular income from our business.

This year, we've paid the majority of invoices within their contractually agreed terms. BT Plc is a signatory to the [Prompt Payment Code](#), but we weren't doing enough to meet its requirements to pay 95% of our invoices within 60 days and our membership to the code was suspended. We agreed an improvement plan with the Chartered Institute of Credit Management in July 2019. BT plc has since improved its 'suppliers paid in 60-days' monthly run rate from around 60% to over 90% during 2019/20. BT plc paid 94.5% of supplier invoices in line with the terms we had agreed with them and aim to comply with local regulations globally.

## Tackling modern slavery

Modern slavery is a threat to human rights on a global scale. We take steps to make sure anyone who works for us or our suppliers freely chooses to do so. And we're using our technology to tackle modern slavery more widely.

### Preventing slavery in our business and supply chain

Our [Modern Slavery Statement](#) explains what we do to prevent modern slavery – including forced, bonded or child labour – within BT and our supply chain. We provide training on this for buyers in our procurement teams and make a recording available to all BT colleagues online.

We assess risk among our suppliers based on the product or service they provide, the country where they operate and the skill level of their workers. Visits to high-risk suppliers let us see working conditions first-hand. We address any concerns with suppliers and we'll cancel our contracts with them if they don't improve.

We're aware of recent allegations of forced labour at Xinjiang, China, involving the supply chains of 17 of our direct suppliers and we're working with these suppliers to investigate.

We'll provide more detail on this in our Modern Slavery Statement for 2019/20.

### Partnering to lead change

We work with other leading companies and experts involved in [Tech Against Trafficking](#) to explore new and better ways to use technology to combat modern slavery.

The Group has so far identified more than 300 existing solutions, and aims to accelerate development of those with the most potential to have a greater impact. For example, the Group ran a tech accelerator programme focused on privacy and data standards issues with the

## Championing human and digital rights continued

[Counter Trafficking Data Collaborative](#) – a global initiative to analyse and access the world's largest global dataset on human trafficking victims – to improve their ability to scale further.

We share our experience to inform emerging policy on human trafficking and modern slavery. We met with the new Independent Anti-Slavery Commissioner to discuss how businesses can become more engaged on this issue. And we responded to the consultation on section 54 of the Modern Slavery Act, which requires certain organisations to develop a slavery and human trafficking statement each year.

Our partnership with the anti-slavery charity [Unseen](#) continued this year. Unseen runs the UK Modern Slavery Helpline and Resource Centre, offering 24/7 advice and support to anyone who calls. During 2019, the Modern Slavery Helpline has taken over 9,000 calls, online reports, and contacts via the Unseen app, indicating more than 4,700 potential victims of modern slavery. Almost 50% of modern slavery cases reported to the Helpline were related to those in situations of forced labour, from across a diverse range of sectors. Some UK police forces and businesses are also using the Unseen app we helped develop last year to support frontline officers and workers in identifying and responding to potential cases of modern slavery.

## Protecting privacy and free expression

As a network and service provider, it's important to keep our customers' information safe so they can communicate freely. By safeguarding our customers' privacy and security online, we in turn support their right to free expression.

### Safeguarding our customers' privacy

We use a privacy impact assessment tool to build privacy into the design of new products or services. And we closely monitor and manage cybersecurity threats to keep our networks, our customers and their data, secure and private (see [page 19](#)). For example, this year we trialled new technology designed to protect information about which websites a user visits by encrypting the website name as it passes over the internet.

We also make sure all our colleagues understand their role in data security and what to do if there's a breach.

### Balancing privacy and government investigatory powers

In certain situations, authorities can legally override the right to privacy because they need access to people's data or communications to help fight serious crime, or for other reasons relating to national security. The government has to find the right balance between protecting the security of all its citizens and the rights to privacy and free expression of individuals.

We're legally obliged to provide information requested under these investigatory powers. But we have processes in place to ensure these requests are properly assessed, and we seek clarification if we have questions about what we're being asked to provide or the legal validity of the request.

Our Board-level [Investigatory Powers Governance Committee](#) oversees all our activity in this area, and their terms of reference are publicly available on our website.

We work with other tech companies and human rights organisations to understand and respond to evolving challenges in this area through the [Global Network Initiative \(GNI\)](#). We're committed to the GNI [Principles on Freedom of Expression and Privacy](#) and this year we assessed our performance against these in order to present our findings to the GNI Board.

We provide a summary of the lawful interception and data disclosure requests received in 2019 by country in the Privacy and free expression section of the [appendix](#).

We provide more details about the types of requests and how we handle them, together with data from the previous year, in our [Privacy and Free Expression Report 2019](#).

### Addressing online harms and illegal content

We support people's right to express themselves. So we won't block access to material online unless it's illegal, such as images of child sexual abuse flagged by the Internet Watch Foundation. We provide data about the material and sites we've blocked in the UK in the [appendix](#). Our [Privacy and Free Expression Report 2019](#) explains more about these complex issues and how we approach them.

We welcome the UK Government's recent focus on tackling online harms and keeping users safe whilst using online platforms and services. We also support the proposal for an independent regulator on the issue.

We've contributed to this debate through consultations and dialogue with key industry and government stakeholders, including responding to the Government's consultation on online harms.

We've also engaged on the impact of specific online harms, partnering with the Royal Society of Arts and the Department for Culture, Media and Sport to [investigate](#) the impact of online disinformation on democracy and society, and explore approaches to mitigate harm.

This year, we renewed our partnership with the [Marie Collins Foundation \(MCF\)](#), which supports children and their families who have been harmed or abused online. We funded their [CLICK: Path to Protection](#) service to train frontline professionals to carry out more effective interventions with victims of abuse. We also gave evidence to the ongoing public independent [inquiry](#) into child sexual abuse and exploitation facilitated by the internet.

We also offer parental controls for our products and work with Internet Matters to help parents keep their children safe online (see [page 12](#)).

“

The support we've received from BT over the past five years has enabled us to meet the recovery needs of many children and young people who have been harmed online, through the promotion and delivery of our [Click: Path to Protection](#) training programme for professionals. BT has doubled the funding for this project for a further three years in recognition of the impact our work has on upskilling professionals to better identify, understand and respond to child victims of online harm.



**Tink Palmer**  
CEO, Marie Collins Foundation



## Championing human and digital rights continued

### Securing our networks

We want people to be able to make the most of technology and realise their rights online. To do so they need to feel safe. We need to secure our network from threats and we want our customers to have the knowledge and tools to protect themselves, their families and their businesses online.

We provide [home](#) and [business](#) customers with tips to stay safe online and protect their data and files. Products like BT Virus Protect and BT Web Protect help protect our customers from viruses, scams, identity theft and phishing attacks.

We're also using our security expertise to support customers through our new Security Advisory Services. It will offer strategic security guidance and solutions to organisations around the world to help them navigate today's complex cybersecurity landscape.

#### Managing cybersecurity risks

Behind the scenes, we work around the clock to monitor risks to our customers' devices. Around 3,000 colleagues on the global BT Security team are supported by 24/7 automated security systems. Our security council is responsible for managing cybersecurity risks and reports to our *Executive Committee*.

This year, we used artificial intelligence (AI) to anticipate emerging threats and help protect the UK from up to 4,000 cyberattacks a day. We also carry out due diligence to check our cloud providers meet the latest industry security standards.

Our security teams completed over 215,000 hours of training this year to maintain their effectiveness. And we're bringing in new talent to build essential cyberskills for the future. This year, 36 apprentices and 116 graduates joined the BT Security team. We also recruit ex-armed forces personnel with transferable skills through our Military Cyber Security recruitment programme.

To broaden awareness of cybersecurity risks, we publish data on the number and type of threats we're detecting through our [Cyber Index](#) website. This year, we blocked on average over 196m connections to malware sites every month.

#### Enabling a safer connected world

Cybercrime is an issue without borders. Tackling it effectively requires national and global partnership.

We work closely with the National Cyber Security Centre (NCSC) and its Active Cyber Defence programme to help make the UK safe for citizens and businesses to operate online. We continue to share information about threats to security and privacy with NCSC, and with law enforcement agencies such as Europol and Interpol, to combat cybercrime in the UK and beyond.

BT was the first communications provider in the world to start sharing information about malicious software and websites with peers. And we've partnered with the NCSC to create a free online platform to enable others to do the same.

This year, we contributed to the Cybercrime [Prevention Principles](#) for Internet Service Providers, published through the World Economic Forum Platform for Shaping the Future of Cybersecurity and Digital Trust.

### Engaging in emerging issues

We work with others to stay ahead of emerging issues and understand potential implications for human and digital rights. Being part of the debate helps us prepare for new opportunities and challenges – and take action.

#### Covid-19 response

We are supporting a range of national public health efforts against Covid-19. At the Government's request, this includes providing a limited amount of aggregated and deidentified network data such as generalised patterns in the movement of people to assist with planning the public response to Covid-19.

#### Using artificial intelligence (AI) responsibly

AI holds great promise. It could help to tackle some of the world's biggest challenges, from climate change to cancer care. At BT, we already use AI for things like tackling nuisance calls, detecting cyber threats and network planning. We're also exploring other uses like modelling our energy consumption to support our journey to become a net zero carbon emissions business.

But we need to understand any potential negative impacts of AI too and explore the ethical questions it raises. How do we make sure the decisions made by AI systems aren't biased towards some people? How do we prevent our networks being used for unethical AI applications? And how will AI impact jobs in the future?

This year, we set up a Responsible AI Working Group. It's tasked with exploring the risks and opportunities of AI technology for our business and with developing a responsible approach to AI that respects human rights throughout our value chain.

We also work with others to help develop best practice. We're part of industry working groups on digital and AI ethics – like [techUK](#), [Digital Catapult](#) and the [Digital Leadership Forum](#) – and we sponsor research on machine learning at Massachusetts Institute of Technology.

We take part in public debates about AI to help make sure any new rules or standards are fit for purpose and enable responsible innovation. This year, we responded to consultations on proposals by the UK Information Commissioner's Office and the Office for AI. We also gave input on new and emerging digital technologies and human rights to the Advisory Committee of the UN Human Rights Council. And our human rights team spoke at events on AI and human rights, including RightsCon 2019.

#### Safeguarding human rights in sports broadcasting

Human rights are as relevant on the pitch as they are online. But there's more to be done to make sure rights are respected and supported in the world of sport. Broadcasters like us have an important role to play.

We're on the advisory council of the Centre for Sport and Human Rights. We also gave evidence to the All-Party Parliamentary Group on Sport, Modern Slavery and Human Rights this year, sharing our approach, progress, challenges and opportunities to tackle human rights issues through our broadcasting.



**Jake Humphrey** highlights human rights issues during commentary on the 2019 UEFA Europa League Final.