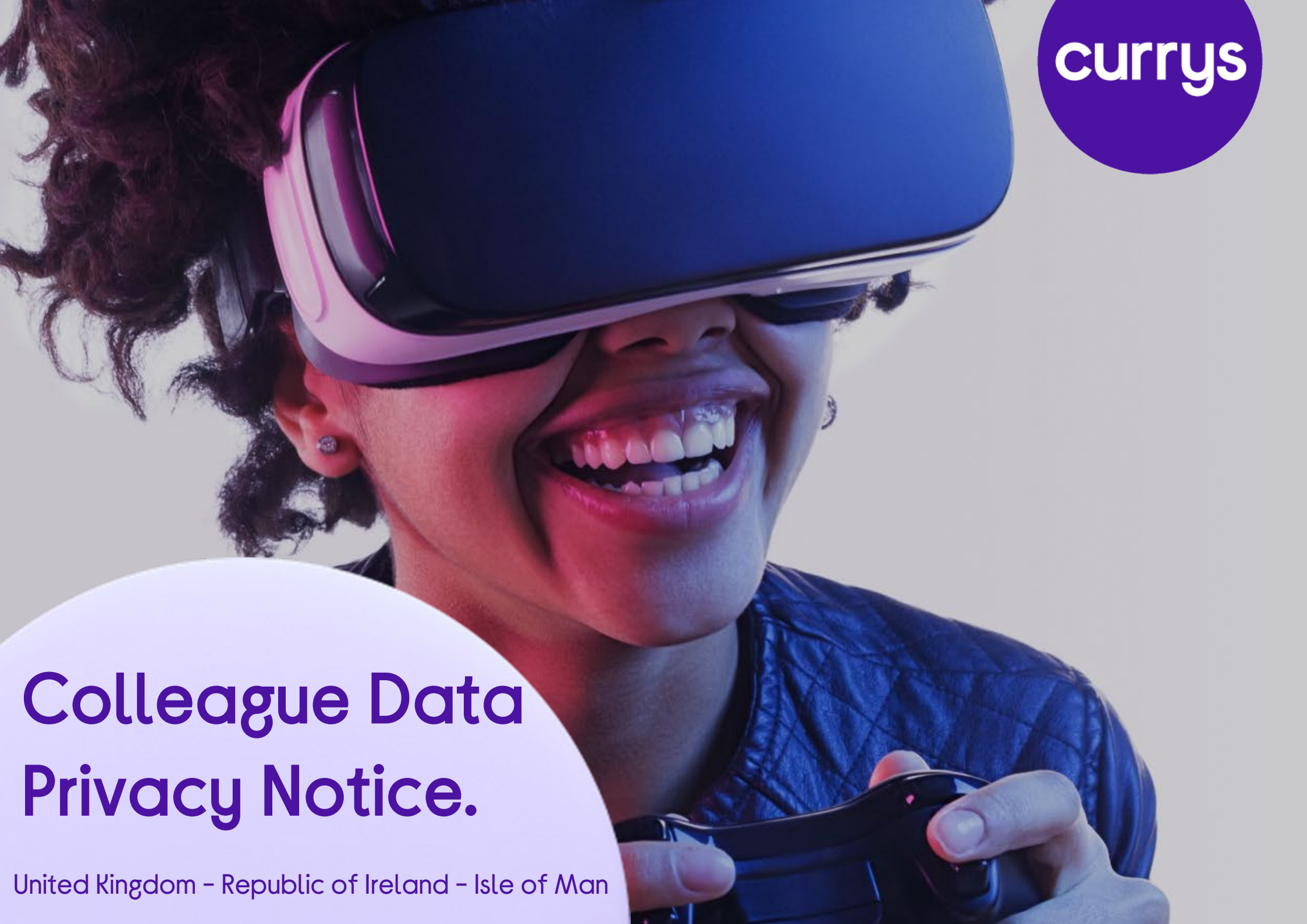
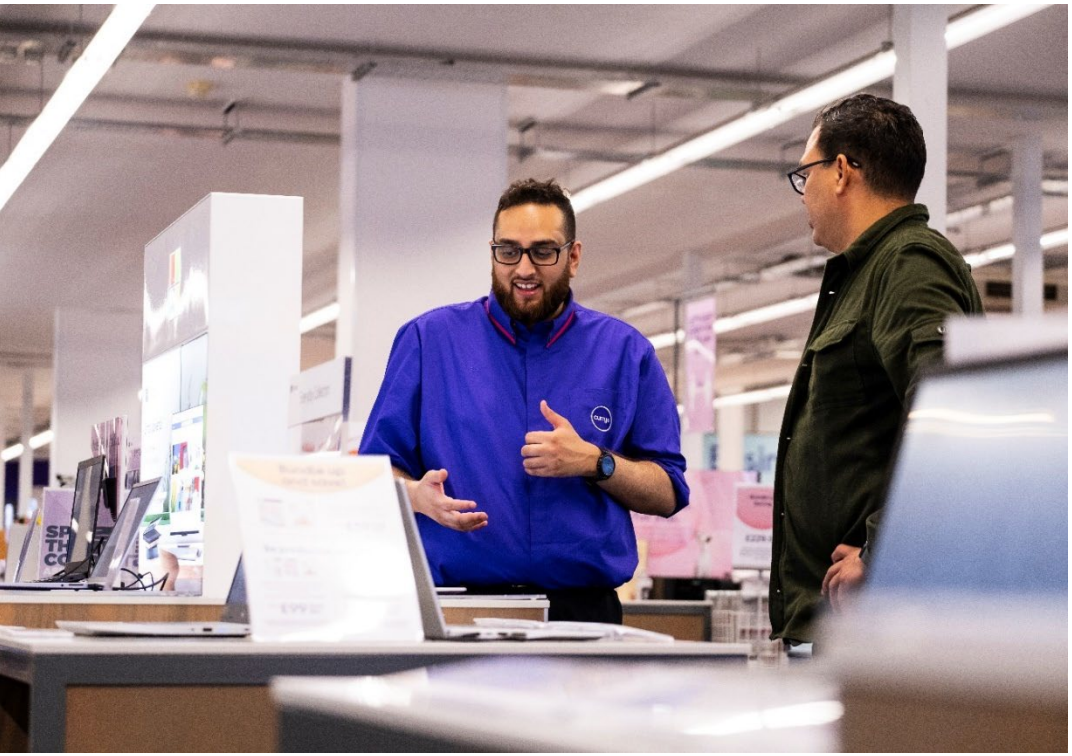


currys

Colleague Data Privacy Notice.

United Kingdom - Republic of Ireland - Isle of Man

Contents



1. Introduction

As one of our Colleagues, we collect, process and store personal information about you to manage the employment relationship between us. We are committed to being transparent about how we collect and use your information.

This privacy notice helps you understand our use of your personal information during and after your time with us. It explains why we collect it, what we do with it and the choices you have, including how to access and update your information.

This privacy notice applies to our employees across our business in the United Kingdom, Republic of Ireland and Isle of Man. Depending on the context, many parts will also apply to those who are not our employees but are engaged by or work for us in some capacity (for example, contractors, agency workers or employees of outsourced service partners). To refer to either, this notice uses the term "**Colleagues**".

Some parts of this notice will also be relevant to our former Colleagues and to the next of kin, family or dependants of our Colleagues.

We have a separate notice which covers personal information collected for potential candidates for employment. This is available on our careers website.

This notice does not form part of any contract of employment or contract to provide services. It may be updated from time to time.

2. Who we are

Currys plc is a leading omnichannel retailer of technology products and services, operating through online and 830 stores in 8 countries. We help everyone enjoy amazing technology, however they choose to shop with us.

As one of our Colleagues, you will be employed by or provide services to Currys plc or one of our group companies (the "**Currys Group**"), namely Currys Group Limited (or Currys Ireland Limited in the Republic of Ireland).

Your personal information may be used by Currys plc or one of our group companies as a data controller or data processor in certain circumstances. For simplicity, in this notice we use "we", "us", "our" to mean the company within Currys Group handling your personal information.

3. Your Security

Our IT systems are protected to make sure that unauthorised or unlawful processing, accidental loss, damage to or destruction of personal information does not occur. Only authorised personnel of Currys Group and of our assured third-party service partners are given access to personal information, and these Colleagues and partners are required to treat this information as confidential.

4. What personal information

Your personal information is any information from which you can be identified. It does not include anonymous information where identity has been removed.

We may handle a range of your personal information, from your name and contact details, to your immigration status, job history, work performance, bank account details, disciplinary records as well as other types of information. You can find examples of personal information we may handle at **Appendix 1**.

You may also be referred to in company documents and records that are produced by you and other Colleagues while carrying out your role.

5. How we obtain personal information

Most of the personal information we handle will have come directly from you (for example, information you shared with us during the recruitment process).

Some personal information may come from other internal sources, such as your manager, other Colleagues or our IT systems. In some cases, we may obtain personal information from external sources, such as referees, background check providers, members of the public, our service partners, government bodies or public sources such as social media.

Personal Information will be stored in a range of different places, including in your personnel file and IT systems operated by us and our service partners.

6. How we use personal information

We use your personal information to enable us to run our business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, while you are working for us, when your employment ends and after you have left. You can find further examples of how we use personal information at **Appendix 2**.

We will only use your personal information for the purposes described in this privacy notice unless we reasonably need to use it for another purpose and that purpose is compatible with the original purposes or as required or permitted by law.

7. Our legal grounds for using personal information

Our use of your personal information will always also be in accordance with the law.

The most common legal ground under which we will use your personal information is where this is needed for **legitimate interests** pursued by us. Our legitimate interests relate to the effective and successful running of our business.

Examples of our legitimate interests

- Running our business efficiently and effectively
- Keeping Colleagues, customers and the public safe
- Furthering our company values
- Managing our workforce including before, during and after employment
- Enabling our workforce to work efficiently and effectively
- Maintaining Colleague and customer engagement
- Implementing our company policies
- Meeting our business (including financial) objectives
- Marketing and promoting our business
- Organisational effectiveness
- Protecting our business assets
- Preventing, detecting and addressing criminality or other malpractice or misconduct
- Operating effective and secure IT systems
- Promoting inclusion and diversity
- Managing and keeping safe and secure our business locations
- Furthering our environmental, social and governance goals
- Running our business compliantly and meeting our legal obligations
- Keeping up-to-date and accurate records
- Defending our legal rights

This is not an exhaustive list

Other common legal grounds under which we may use your personal information include:

- where needed for the performance of the contract between us. For example, to pay your salary
- where needed to comply with a legal obligation, particularly as your employer. For example, legal obligations relating to deducting tax and social security, health and safety and statutory rights like maternity leave
- where needed for legal proceedings

Less commonly, we may use personal information where we need to protect the interests of others, including you or members of the public or for legitimate interests pursued by third parties.

In limited cases, we may rely on an exemption in Schedule 2 of the Data Protection Act 2018 (or equivalent provisions in the Republic of Ireland) to justify our use of personal information.

8. Special Categories of personal information

The personal information we handle may include information of a more sensitive nature, known as Special Categories of personal information.

Special Categories of personal information include racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health; sex life and sexual orientation.

Examples of how we may use Special Categories of personal information include:

- handling Colleague grievances, disciplinaries and other types of complaints where the subject matter includes Special Categories of personal information, for example, allegations of sexual harassment or disability-related discrimination
- using information relating to your health in different situations, for example, to assess fitness to work, make reasonable adjustments if you have a disability, to administer our sickness absence and pay policies, make referrals to Occupational Health and provide health-related Colleague benefits
- using health information in the course of addressing substance abuse issues under our Drugs and Alcohol policy, including carrying out drugs and alcohol testing (both internal testing and testing by third-party test providers)
- collecting inclusion and diversity information as part of our equal opportunities monitoring activities, conducting relevant analysis within our business and for statutory reporting purposes
- maintaining a safe working environment by operating access control systems which utilise biometric data, such as fingerprint or facial recognition technology

The use of Special Categories of personal information requires additional safeguards. These are explained in Section 10 below.

9. Criminal Records information

The personal information we handle may include Criminal Records information, which is information that relates to criminal offences or convictions, including allegations of criminal behaviour. We may obtain Criminal Records information directly from you, through law enforcement, via criminal record checks or other means (for example, from another Colleague, a customer, a member of the public, a regulator or a public source such as social media).

We may handle Criminal Records information in different ways, for example:

- we may ask about your criminal record and carry out criminal record checks where we consider this necessary for the role or if required by law. This may happen during the recruitment process and on an ongoing basis during your time with us
- we may learn of a criminal investigation, prosecution or conviction of a Colleague directly from the Colleague or from another source. We will use this information to consider the impact this may have on the Colleague's role
- we operate a confidential Colleague hotline, through which we may receive reports of malpractice impacting our business which may amount to Criminal Records information and/or Special Category information. We may also receive reports from other sources
- we may investigate allegations which amount to Criminal Records information and take appropriate action
- we may handle personal information including Criminal Records information in the course of our loss prevention activities, including sharing information with third parties and accessing fraud and theft prevention databases and resources to prevent and detect loss of stock, other business assets and associated criminality
- we may share Criminal Records information with law enforcement, regulators, professional advisers and others where legally required or permitted. This includes where requests are made of us for information or where we determine it appropriate voluntarily to share information, for example, to investigate or stop suspected criminality

The use of Criminal Records information requires additional safeguards. These are explained in Section 10 below.

10. Additional Safeguards

The use of Special Category or Criminal Records information requires us to have an additional legal ground for using the information.

The most common additional legal ground we rely on is where the use of Special Category or Criminal Records information is needed to

carry out our obligations or exercise our rights in the context of employment. This ground covers the use of Special Category or Criminal Records information in a range of scenarios, for example:

- complying with immigration laws, such as the requirement to check a Colleague's right to work
- complying with employment laws such as those relating to the effective management of complaints, avoiding unlawful dismissals, anti-discrimination legislation, statutory leave and sick pay, trade unions and collective bargaining and our duty of care as an employer
- complying with regulatory rules relating to our workforce
- complying with our various legal duties under health and safety law and maintaining a safe environment for Colleagues and customers alike

Other legal grounds under which we may use Special Category or Criminal Records information include where needed for the purposes of:

- occupational medicine
- assessing working capacity
- equal opportunities monitoring
- operating our pension scheme
- preventing and detecting unlawful acts
- protecting the public against dishonesty, malpractice or other seriously improper conduct, unfitness or incompetence
- meeting regulatory requirements relating to unlawful acts and dishonesty

Less common legal grounds under which we may use Special Category or Criminal Records information include to protect your (or another person's) vital interests where you (or they) are physically or legally incapable of giving consent (for example in emergency situations), the establishment, exercise or defence of legal claims, safeguarding the interests of children or vulnerable people, public health and where you have already made the information public.

The above legal grounds apply in the United Kingdom. We rely on equivalent or similar legal grounds in the Republic of Ireland and Isle of Man.

We have in place an Appropriate Policy Document (available on request and on our Intranet) which explains how we comply with data protection law when using Special Category or Criminal Records information.

11. Do we need your consent

Generally, we do not need your consent to use your personal information. There may be occasions where we request your consent, and we will explain why we need it at the time. Where we use personal information based on your consent, you have the right to withdraw that consent at any time.

12. Automated decision-making

An automated decision is a decision affecting an individual made solely through automated means (for example, by a computer system).

While working for us, you will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We may use automated decision-making in the recruitment process, for example, we may use online candidate assessments to enable us to narrow down large numbers of applications. This is explained in more detail in our Recruitment Privacy Notice (available on our careers website).

13. Information technology administration and monitoring

We use IT systems across our business, operated by us and our service partners.

We and/or our service partners may need your personal information to grant, administer and terminate your access to our IT systems. Your personal information may also be required so that we can perform other IT-related activities such as reporting, managing and resolving faults or other IT issues you may encounter when doing your job, and for the administration, support, development, testing, management and maintenance of our IT systems.

We monitor, and access information within, our IT systems for a range of purposes including analytics, security, investigations (including into complaints or allegations of misconduct) and where required or permitted by law. We may monitor, analyse and access network traffic to prevent, detect and investigate suspicious, malicious or illegal activity, including authorised access to or disclosure of Currys Information. All information placed on our IT systems belongs to us and may be accessed. You should not store, send or receive any information which you wish to keep private on our IT systems, as it could be accessed at any time, including after you have left us.

We may carry out covert monitoring of Colleagues in exceptional circumstances, for example, where there is a suspicion of fraud, theft or other criminality and no less intrusive way to investigate.

14. CCTV

We use CCTV across our business, including in all of our stores. We use it to help keep our customers and Colleagues safe, as well as to protect business assets. CCTV footage might also be used as part of an investigation or to monitor compliance with health and safety measures.

15. Driving for work

Many of our Colleagues drive for work purposes and may do so using one of our commercial vehicles, a company car or their own vehicle.

We may handle driving-related personal information in a range of ways to ensure that those driving for work do so in a safe, compliant and efficient way. For example:

- we may carry out periodic driving licence checks
- for company car drivers, personal information may be recorded in company car ordering systems and we may arrange a fuel card facility (provided by a third party) on their behalf. We may also handle the personal information of any nominated drivers
- drivers of our commercial vehicles may be subject to additional checks and assessments
- the location and routes taken by our commercial vehicles may be tracked and recorded. Commercial vehicles may also be fitted with audio-visual recording devices, including forward, rear and in-cab facing cameras with microphones
- our company cars and commercial vehicles may be fitted with tachograph technologies, recording information such as driving time, speed, distance and location
- we may record mileage and related information for the purposes of driving-related expenses claims
- we may be required to report road traffic accidents to the Traffic Commissioners for Great Britain

16. Colleague engagement platforms and use of Colleague images

Colleague engagement is about ensuring our Colleagues feel happy and fulfilled at work and fostering engagement is a key priority for us.

One of the ways we do this is by making available internal engagement platforms. This may take the form of instant messaging services or an internal-facing social media platform, allowing Colleagues to connect with each other, share their working experiences and receive business updates and communicate.

These platforms may involve the use of personal information, for example, name, job details, contact details and information included within posts by us or Colleagues. This may include images (and videos) of Colleagues – for example, performing work-related activities, receiving awards, sharing work experiences or attending training sessions and other events.

Personal information uploaded onto these platforms will be viewable by all Colleagues with access to them. If you leave us, you should review your posts and delete any content you do not wish to remain viewable to others. We monitor use of these platforms as explained in Section 13 above.

Images (including video) of Colleagues may also be captured and used internally for the purposes of Colleague engagement in other ways, for example:

- senior managers give business and performance updates during 'town halls' and similar events. These are often filmed (including the audience) and made available for Colleagues to view
- filming may take place or photographs may be taken in our business locations
- internal noticeboards may feature Colleague images, such as 'Colleague of the month' notifications

We may also use Colleague images for organisational reasons, for example, in internal directories or profiles.

From time to time, Colleague images may be used to promote our business externally to customers. This might be done, for example, in a marketing campaign. Such activity will be overseen by our central marketing teams and Colleagues will be asked for their agreement.

17. Public health events

In the case of a public health event, such as a pandemic, we may introduce measures which involve additional uses of your personal information. We will do this to keep our Colleagues, customers and others who interact with our business safe and comply with our legal obligations. Measures may include:

- facilitating shielding and other relevant measures for vulnerable Colleagues
- managing self-isolation, absences and international travel restrictions
- internal infection tracking and disease control
- complying with our reporting obligations to public health authorities
- CCTV monitoring of compliance with social distancing and safety measures
- temperature / symptoms checking
- testing of Colleagues where necessary (for example, in areas of particular risk, due to multiple infections or due to the risk profile of particular roles), which may be provided via a third-party testing provider
- analytics including vaccination status

Where relevant, these measures may include processing of personal information including health-related information such as test results and symptoms or other health conditions, vaccination status and other Special Categories of personal information including ethnicity and gender where required under public health reporting obligations.

18. Who has access to your personal information

Our policy is that only those who have a legitimate need to access your personal information will be able to do so. For example, your line

manager may hold records on performance, notes of one-to-one interviews, emergency contact numbers etc. They will also be able to access information we hold about you on HR systems, including general job-related information, current pay, and absence history.

The People Team, Finance and other professionals will also have access to information about you, for example, to enable them to manage the needs of the business, provide specialist support to management and to calculate pay and bonus entitlements.

Where you are asked to provide equal opportunities monitoring information, and you provide it, access to this is restricted to a much smaller group who need to know this information to carry out our diversity and inclusion activities or meet our legal obligations.

Certain basic personal information, such as your name, location, job title, contact information and any published skills and experience may be accessible to other Colleagues via our Intranet, Colleague directories and organisational charts.

19. Who we share your personal information with

We share personal information within Currys Group. Members of Currys Group that receive this information are not authorised to use or disclose the information except as provided in this privacy notice.

Other than as mentioned below and elsewhere in this privacy notice, we will only disclose information about you to third parties if we are legally obliged or permitted to do so.

Our service partners

We work with a number of service partners to enable us to run our business effectively and this can include carrying out activities described in this privacy notice on our behalf.

Our use of your personal information as set out in this privacy notice may include sharing personal information with our service partners (and their sub-contractors), to enable us to manage our relationship with you and run our business effectively.

This includes suppliers, professional advisers, auditors, insurers, pension and other Colleague benefits providers and other third parties. Further examples of service partners we may share information with is included at **Appendix 3**.

When we engage new or replacement service partners, we or our previous service partner may transfer personal information to them to enable the provision of the relevant service. We always require our service partners to meet our standards on the processing of personal information and security.

Our regulators

We are regulated by a range of bodies, which set the rules we must follow to run our business compliantly. In the United Kingdom, this includes the Financial Conduct Authority (the "**FCA**"), The Information Commissioner's Office, the Competition and Markets Authority, the Office of Communications and the Health and Safety Executive.

It may be necessary for us to share personal information with our regulators, for example, during an investigation or enforcement action or to comply with reporting obligations and other rules set by the relevant regulator.

For example, we are subject to the FCA's Senior Managers and Certification Regime, which may involve sharing personal information with the FCA concerning Colleagues' work history, role details and fitness and propriety. Our Colleagues are also required to comply with Conduct Rules set by the FCA and details of any breaches of these rules may need to be reported to the FCA.

Other organisations and individuals

We may transfer your personal information to other third parties in certain scenarios. For example, we may share information with:

- government and other relevant bodies to fulfil our statutory responsibilities. For example, providing salary and tax data to HM Revenue & Customs
- your next of kin, emergency contact or other representatives acting on your behalf in certain scenarios, for example, in an emergency, where you are incapacitated or are otherwise unable to communicate with us
- third-party commercial partners, for example, because the work you do is relevant to the commercial arrangement between us
- third parties in the context of our pre-employment checks and Colleague vetting activities, for example, bodies providing criminal record checks or previous employers and educational institutions
- learning and training providers, for example, in the case of apprentices
- third parties managing buildings in which Colleagues carry out work for us, for example, for access control, security and safety purposes
- law enforcement
- third parties in the context of a potential sale of some or all of our business / a transfer of undertakings
- our customers, where this is relevant to your role
- a third party you have given us your consent to disclose to

We may also be legally obliged to share information, for example, in the context of disclosure of evidence during legal proceedings or in response to a valid legal disclosure request.

Employment references

If you apply for another job, we may be asked by your prospective employer to provide an employment reference in respect of you. This may involve us confirming your job title and dates of employment. All employment reference requests should be made to: people.place@currys.co.uk

In respect of certain roles regulated by the FCA, we may be required to seek or provide a more detailed reference about you, known as a Regulatory Reference, which may include additional personal information, for example, work history and any conduct issues.

Similarly, we may receive requests for information about you from other third parties, such as your legal representatives, benefit agencies and insurers. Where we are satisfied the request has been made at your instigation, we will share information in line with our policies on responding to such requests.

20. Transfers of personal information outside of the UK / EEA

Generally, we will use and store your personal information in the United Kingdom and the European Economic Area (for example, the Republic of Ireland), as this is where our business operates.

In limited cases, we may transfer your personal information outside of the United Kingdom or the European Economic Area. This may be because, for example, a service partner is based outside of these areas.

Where we transfer personal information to a third country which is not recognised to have an equivalent level of protection for personal information, we will take additional measures to ensure that personal information is protected to our standards. This can include implementing additional safeguards, including contractual measures (known as Standard Contractual Clauses) and additional security measures.

21. Personal information of your family and next of kin

We may use personal information about your family and next of kin, such as names and contact details. We will use their information for the purposes set in this privacy notice, most commonly, to provide employment-related benefits or in an emergency. We will use their information in a manner consistent with this privacy notice and as permitted by law.

22. Keeping your information accurate and up-to-date

It is important that the personal information we hold about you is accurate and up-to-date.

You are responsible for providing accurate information and updating the information when changes occur. You should review your information in SuccessFactors, at least annually, for accuracy, and provide updates by using the self-service facilities. If information is incorrect and you are unable to change the information through SuccessFactors, please contact the People Services Team.

23. Your Rights

You have several rights under data protection laws in relation to our use of your personal information.

Access to information held about you

You have the right to request a copy of the personal information we hold about you. This is sometimes called a **Data Subject Access Request**. There are various exemptions to this right which may entitle us to withhold disclosure of personal information, for example, where it is mixed with the personal information of other individuals, and it would be unreasonable to disclose it.

Where we agree that the personal information you have requested is not exempt, we will generally provide it to you free of charge. We may charge a fee or refuse a request if it is manifestly unfounded or excessive.

Correction of your personal information

If any of the personal information we hold about you is inaccurate or out of date, you can request that it be corrected or updated. You can also update some of your personal information yourself via our Intranet.

Right to object, erasure, restriction and data portability

In certain circumstances, you have the right to object to our use of your personal information where we are relying on a legitimate interest, request erasure of your personal information, request the restriction of our use of your personal information and request the transfer of your personal information to another party.

When we consider your request, there may be reasons why we cannot comply, for example, where it is necessary for our use of personal information to continue and this is permitted by law.

How to make a request

If you would like to exercise any of these rights, please email: colleagueDSAR@currys.co.uk

When you make your request, you will be asked to provide appropriate identification documents as part of your application. We may also seek further information from you to help us consider your request. Except in complex cases or where we need more information from you to verify your identity or clarify your request, we will respond to you within one month.

24. How long Currys retains personal information

We will continue to hold your personal information for as long as we reasonably need to, having regard to our purpose for using the information. Generally, for employment-related records containing personal information, this means keeping records for as long as you are employed / engaged by us, and then for a further period of 6 - 7 years after you have left.

We may keep records for shorter or longer periods if we are required to do so legally or have assessed it to be reasonably necessary.

25. Contact

Any queries regarding this privacy notice should be emailed to people.place@currys.co.uk

26. Complaining to the Data Protection Regulator

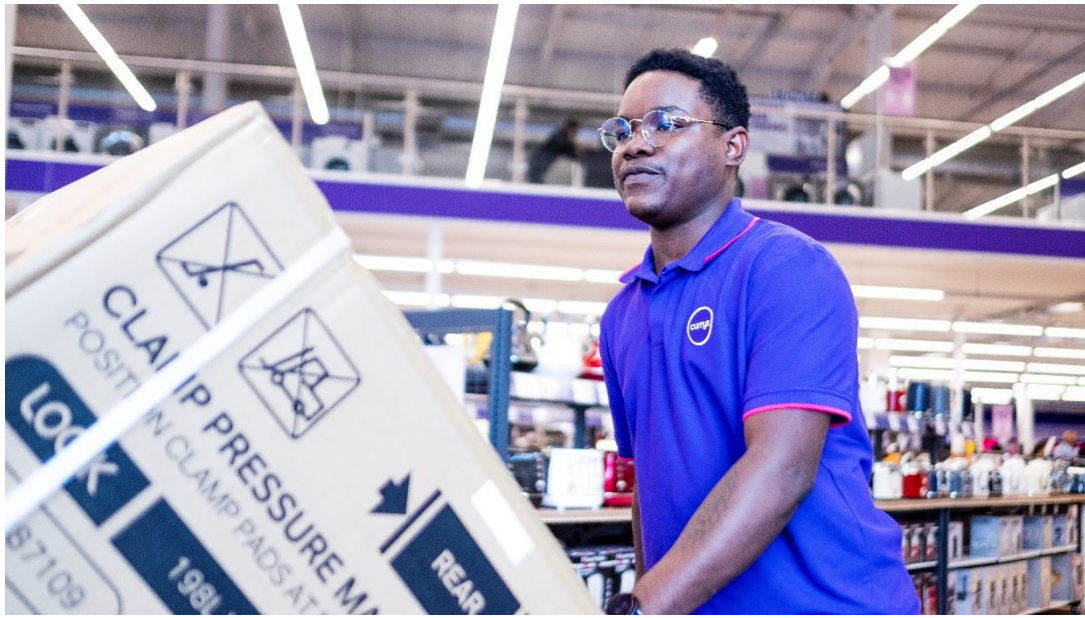
If you are concerned about the way we have processed your personal information, you can get in touch with our Data Protection Officer Team, who can be contacted via dpo@currys.co.uk

Alternatively, you are entitled to complain to your local data protection regulator:

- **In the UK:** The Information Commissioner's Office. For further details, please visit: **www.ico.org.uk**
- **In the Republic of Ireland:** The Data Protection Commission. For further details, please visit: **www.dataprotection.ie**
- **In the Isle of Man:** The Isle of Man Information Commissioner. For further details, please visit: **www.inforights.im**

27. Updates to this privacy notice

We may review this privacy notice from time to time and any changes will be notified to you by posting an updated version on our Intranet and/or by contacting you by email.



Appendix 1

This table sets out examples of personal information we may handle, including records which may contain personal information

Basic information
- names, title
- contact details (e.g. addresses, phone numbers, email addresses)
- date of birth, age, gender, pronouns
- marital status and details of any spouse/partner/dependants
- Identification (e.g. passport, birth / marriage certificate, utility bills)
- emergency / next of kin details

Recruitment and suitability
- information from CV / application form / LinkedIn
- previous employment
- education, skills, qualifications, languages
- salary expectations and previous contract information (e.g. notice period, restrictive covenants, pay and benefits)
- hobbies / interests
- professional memberships
- willingness to travel / relocate
- other information provided or created (e.g. during interview, via agency, assessments)

Vetting and conflicts
- information from pre-employment checks
- credit history
- reasons for leaving past employment
- disciplinary history
- outside interests, employment, engagements or directorships
- conflict of interests

Immigration and nationality
- right to work checks
- visas, IDs, applications, correspondence
- nationality, place of birth, languages

Job and contract
- job details (e.g. title, description, grade, line management)
- payroll number / other IDs / cost centre
- employment status
- promotions / transfers / internal job applications / work history
- contract type (e.g. permanent, fixed-term, agency, consultancy, secondment)
- contract terms (e.g. location, notice period, hours)
- supplemental contractual arrangements

Attendance and leave
- hours of work / shift pattern
- time and attendance information
- information relating to all types of leave (e.g. holiday, maternity, paternity, adoption, shared parental, emergency, dependants, compassionate, furlough, special, unpaid) and associated administration

Health
- pre-employment medical assessments
- medical conditions, including disabilities and other disclosed health information
- accommodations and adjustments
- testing information (including for drugs and alcohol and results)
- vaccination status
- sickness absence (e.g. dates, reasons for absence, fit notes)
- diagnosis and prognosis information, including medical reports
- referrals to and communications with Occupational Health including specialist referrals

Driving
- driving licence and vehicle registration number
- driving licence checks
- company car details, including nominated drivers and fuel card information
- driving history / offences / assessments
- accident and incident investigations
- company vehicle tracking and monitoring, including tachographs and front, rear and in-cab audio / visual recording devices

Performance and appraisal
- work output information and assessments
- performance management / improvement plans
- appraisal information including objectives, periodic reviews, management opinions, feedback and ratings

People process
- grievances / complaints raised by or involving you
- conduct / disciplinary issues involving you, including investigations

Pay and benefits
- current and previous salary and allowances
- salary review
- bonus, overtime and commission
- participation in Colleague benefit schemes (e.g. pension, life assurance, medical cover, share schemes etc) including cover, policy numbers, selection preferences, dependents / beneficiaries and associated administration

Regulatory
- regulatory status and history, including regulatory references
- registration information
- breach of regulatory rules, including reports to regulators

Health and safety
- accident records, RIDDOR reports and other health and safety records
- risk assessments

Security and IT
- CCTV
- access control (e.g. key card and biometric - finger / handprint and facial recognition), including dates/times of access
- use of IT and other systems, telephone records and other monitoring information and analytics

Criminal Records
- criminal record history
- criminal record checks / disclosures / self-declarations
- conduct issues which amount to Criminal Records information, including investigations
- details of current criminal charges / investigations
- communications / sharing of information with law enforcement, regulators and other bodies

Inclusion and diversity
- information collected pre and during employment relating to racial or ethnic origins, sexual orientation, religious or similar beliefs, health (including disability), social mobility and (in Northern Ireland) community background
- other information disclosed as part of our inclusion and diversity activities

Payroll and expenses
- payroll information (e.g. tax code, payslips, tax and social security deductions, other deductions, bank details, tax file, student loan, payments to be made, submissions to tax authorities)
- expenses details

Training
- training history, including results, completion status, completion date, periodic self-declarations and other analytics
- external learning provider and associated administration

Organisational
- organisation charts / directories
- personal information recorded in business-related materials, including emails, presentations, meeting notes and recordings, succession planning, organisational design, insider lists, customer sales and complaints handling and other business records
- information used in internal company communication and engagement platforms
- gifts and hospitality
- complaints from customers
- information used in company social media platforms
- image / other information in company marketing
- information derived from in-store customer engagement and tracking technologies, mystery shopping and live online sales and repair services

Non-employee Colleagues
- information provided from direct employer, recruitment agency or other relevant intermediaries
- information related to IR35 and other relevant areas of compliance

Leaving
- date and reasons for leaving, including resignation and dismissals
- information from associated processes (e.g. disciplinaries)
- return of property
- redundancy information, including notes of meetings, selection, payment calculations
- termination payments and entitlements
- exit interview information

Other personal information
- information from public social media, such as LinkedIn
- photographs, video and audio
- dietary requirements and other personal preferences
- caring responsibilities and other home and family life information
- volunteering and other activities outside of work
- information used during the bringing or defending of legal or regulatory proceedings and the exercise of legal rights (e.g. data subject access requests)
- information obtained from public sources (e.g. Companies House, public directories, news media etc)
- information used in an emergency
- correspondence with or about you

References and post-employment
- Requests for information about you and our response (e.g. employment references, enquires from government agencies, insurers and other third parties)
- records containing personal information held in accordance with our retention policies

This is not an exhaustive list.

Appendix 2

The following are examples of how we might use Colleague personal information:

- Engaging with prospective Colleagues
- Operating Colleague recruitment and onboarding processes
- Performing pre-employment checks
- Determining the terms on which you work for us and issuing relevant paperwork such as an employment contract
- Operating payroll (or otherwise arranging payment of wages or fees) including making deductions for tax and social security
- Providing and managing work-related benefits
- Providing and managing pension schemes
- Managing the contract between us
- Operating IT systems / tools to enable Colleagues to perform their roles and be engaged
- Business management and planning, including accounting and auditing
- Carrying out commercial activities involving use of Colleague personal information
- Dealing with customer or third-party complaints involving use of Colleague personal information
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and remuneration
- Assessing qualifications for a particular role or task, including decisions about promotions
- Operating a confidential (whistleblowing) hotline
- Operating our company policies
- Preventing, detecting, investigating, reporting and acting against criminality, dishonesty, fraud and other malpractice and misconduct
- Operating our grievance and disciplinary procedures
- Operating compliance programmes, for example, in relation to anti-bribery, gifts and hospitality, mis-selling, vulnerable customers, market abuse, competition law, IR35 and FCA requirements
- Conducting workforce surveys
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Managing driving for work, including our commercial vehicle fleet and company cars
- Operating an apprenticeship or similar programmes
- Providing Colleagues training and career development
- Dealing with legal disputes involving you or other Colleagues
- Ascertaining your fitness to work, managing sickness absence and operating our capability procedure
- Carrying out health and safety risk assessments and managing accidents
- Verifying identity when you access certain services, such as our IT helpdesk
- Carrying out criminal record checks and periodic self-declarations
- Monitoring including of our IT systems and ensuring network and information security, including detecting and preventing unauthorised access, disclosure and malicious software distribution
- Conducting data analytics studies to review and better understand Colleague retention and attrition rates
- Operating access control, CCTV and other security measures
- Equal opportunities monitoring
- Responding to requests for information from prospective employers of current or former Colleagues and from other third parties
- Transferring employment records in the context of a sale of part or all of our business or a TUPE transfer
- Managing our post-employment / engagement relationship
- Maintaining business records

This is not an exhaustive list.

Appendix 3

We may share personal information with third-party providers of:

- IT such as software, communication, security and threat detection, disaster recovery, helpdesk and support services
- Pre-employment checking services, such as references, criminal record and immigration checks
- Job applicant assessment platforms
- Human resources, recruitment, onboarding, payroll, administration and other business process outsourcing
- Supply of labour, including recruitment agencies and delivery partners
- Occupational Health including health checks and onward specialist referrals
- Colleague benefits, such as private medical insurance, life assurance and share incentive schemes
- Colleague benefits selection and management platforms
- Colleague testing services, including drugs and alcohol
- Colleague surveys including results analysis
- Internal Colleague engagement and communication platforms
- Occupational pensions, including trustees and administrators
- Outplacement
- Health and safety assessments and compliance services
- Regulatory compliance platforms, such as a gifts and hospitality register, project and insider lists
- Confidential (whistleblowing) hotline services
- Tax-related assessments, such as in relation to IR35
- Driving-related assessments and administration, including of company cars and fuel card facilities
- Employee Assistance Programme services
- Colleague training, experiences, gifts, competitions and offers
- Online live sales and repair services platforms
- Building and facilities management and security
- Record keeping, archiving and data deletion and destruction services
- Security systems such as CCTV (both fixed and in-vehicle, as well as the storage and processing of footage) and access control
- Mystery shopping
- Insurance cover
- Legal, claims management, banking, accounting, auditing, analytics, investigative and other professional services

This is not an exhaustive list.