Code of Practice for the Application of Driver Licensing Data for Policing and Law Enforcement Purposes
Part A

1. Introduction

1.1. The Driver and Vehicle Licensing Agency (DVLA) is responsible for the registration and licensing of drivers in Great Britain, and in doing so maintains records of all of those who hold or have held DVLA issued full or provisional driving licences, including (additionally) all drivers' endorsements and disqualifications notified to the DVLA.

1.2. The Criminal Justice and Court Services Act 2000, as amended by section 154 of the Crime and Policing Act 2026 together with the Access to Driver Licensing Information Regulations 2026 (SI 2026/xxxx) [1] enable policing and law enforcement agencies to make more effective use of driver licensing data. Police and law enforcement can now use automatically accessed driver licensing information for policing and law enforcement purposes as opposed to just for road traffic matters. The new legislation also clarifies which organisations, and which individuals within the specified law enforcement agencies, can access the data and how they need to behave when so doing.

1.3. As officers no longer always need to approach the DVLA directly to access driving licence data for investigation or prosecution of other matters, policing now has real time access to that data for time sensitive critical investigations such as kidnapping, stalking and searches for vulnerable missing persons. The police can still directly approach the DVLA to dig deeper into a record provided automatically or to consider an application for use for wider purposes where it might be appropriate to seek further advice.

1.4. The legislation also allows the Secretary of State for the Home Department [2] to issue a Code of Practice. This is intended to serve two purposes:

- To enable driver licensing data to be used as an important and useful tool for policing, law enforcement and safeguarding within clear legal and ethical boundaries.
- To provide Parliament and the public with assurance on the integrity of the use of the data.

[1] To be updated when the regulations are laid
[2] Exact mechanism to be agreed between Home Office and DfT

2. Statutory basis of the Code

2.1. The Code has been made under powers in the revised Section 71B of the Criminal Justice and Court Services Act 2000. These permit the Secretary of State (i.e. the Home Secretary) [3] to issue a Code of Practice about the receipt and use of information made available under section 71 of the 2000 Act. It provides statutory guidance on how that driver information is made available by DVLA and how that data should be used by police and law enforcement organisations for policing and crime purposes.

2.2. The Code is an integral part of the overall legislative package which includes the Act itself and the regulations which outline the conditions under which driver licensing information may be made available. It is applicable to all organisations which are accessing driver licensing information from the DVLA. Driver licensing information is defined as information held, in any form, by the DVLA on behalf of the Secretary of State for Transport for the purposes of Part III of the Road Traffic Act 1988. The Code is a publicly available document and should be readily accessible by any persons who wish to consider it.

3. Scope of the Code of Practice

3.1 The Code of Practice applies to all the organisations listed in the legislation. These are referred to as 'Authorised Organisations' in this Code. They are civilian and service police forces within England, Wales, Northern Ireland and Scotland, including the National Crime Agency. The Code also applies to the bodies responsible for the investigation of police complaints (civilian and military). Schedules reflect different legislative and procedural contexts for Scotland and Northern Ireland. The Crown Dependencies and Gibraltar have agreed to observe the Code in their written agreements with DVLA. The Code concerns the use of DVLA data accessed by any current or future process.

3.2 The Code of Practice applies directly to those persons who exercise the power of access as made available through Section 71 of the 2000 Act and who are referred to as the "Authorised Officers". They have an individual responsibility for compliance.

4. Ownership and accountability for the Code

4.1. Ownership and accountability

This Code is owned by Home Secretary with administration and management carried out by the Home Office. The Home Office is accountable for the implementation of the Regulations and the Code and for preparing an Annual Report, to be published on Gov.UK. The Home Office, working with partners, will review and refresh the Code of Practice

[3] Exact mechanism to be determined between Home Office and DfT

as appropriate. The Scottish Government and Department for Justice Northern Ireland have approved the respective schedules below.

5. Code Principles

5.1. Understanding the lawful use and permitted purposes of driver licensing data

Authorised persons must understand the statutory basis on which driver licensing data may be accessed and the purposes for which it may lawfully be used. This includes being clear that access must support a legitimate policing, law enforcement or safeguarding purpose, and that use of the data must remain necessary, proportionate and connected to that purpose.

5.2. Ensuring the appropriate, fair and ethical use of driver licensing data

Driver licensing data must be used in a way that is fair, responsible and consistent with legal and ethical standards. This requires authorised persons and organisations to take proper account of data protection, human rights and equality obligations, and to ensure that the use of data does not result in arbitrary, discriminatory or unjustified interference with individual privacy.

5.3. Providing appropriate training, authorisation and access controls for driver licensing data

Access to driver licensing data must only be granted to appropriately authorised individuals who have received the training, guidance and support needed to use it properly. Organisations should ensure that access arrangements, supervision and refresher learning remain effective so that those using the data understand both the operational value of the information and the safeguards that govern its use.

5.4. Maintaining accountability through regular monitoring, audit and review

There must be clear accountability for how driver licensing data is accessed, used and governed within each authorised organisation. This should be supported by effective monitoring, audit and review arrangements that enable organisations to identify misuse, demonstrate compliance, learn lessons and provide assurance to the Home Office, Parliament and the public.

5.5. Ensuring driver licensing data is shared lawfully, appropriately and only where necessary

Driver licensing data must only be shared onward where this is lawful, necessary and connected to the purpose for which the data was

obtained. Any onward disclosure should be carefully controlled, limited to what is needed, and carried out in a way that protects the integrity of the information and maintains public confidence in its use.

Part B

6. The aims of the Code

6.1. Two aims of the Code

I. providing guidance so that authorised persons can use driver licencing data as an important and useful tool while operating within clear legal and ethical boundaries.
II. providing Parliament and the public with assurance in the integrity of the use of that expanded power by identifying the safeguards that are established and the accountability for ensuring these are effective.

6.2. How these aims are delivered

I. **Promoting understanding**: Enabling greater understanding of the legitimate policing and law enforcement purposes for processing driver data. Policing and law enforcement personnel who access the data develop a clear understanding of how driver data can be appropriately used to support the prevention, investigation, detection or prosecution of criminal offences, to protect the public and to safeguard vulnerable people.
II. **Promoting fairness**: Seeking to ensure that driver licensing information is not used in a discriminatory or unethical manner. The Code describes the safeguards that protect data and privacy interests. The operation of the legislative provision, regulation and Code is reported upon annually so the public can be reassured that it is consistent with the law and evolving human rights, data protection and ethical standards.
III. **Promoting accountability**: Ensuring that the use of driver data has a clear line of responsibility. Each organisation accessing driver data from the DVLA demonstrate that they understand and comply with the safeguards that support the purposes for which they may use that personal data, including compliance with data protection legislation. The Code encourages transparency in how data that is supplied by DVLA is applied for law enforcement, policing and safeguarding purposes in ways that are both necessary and proportionate. The external mechanisms for oversight and accountability will be clarified.
IV. **Enabling performance**: Facilitating performance by requiring clear management structures, specifying audit requirements and providing learning and guidance for users and by a requirement for organisations to proactively support relevant continuing professional development among all users.

7. Promoting understanding

7.1 All authorised persons must have a clear understanding of the legitimate policing and law enforcement purposes for processing driver data by law enforcement. A specific package of learning and guidance should accompany this Code to ensure all current and potential users of driver licensing information are clear as to the appropriate circumstances in which data gathered by the DVLA for road traffic purposes may be applied to support the prevention, investigation, detection or prosecution of criminal offences, to protect the public and to safeguard vulnerable people. It is essential that this is understood to be consistent with the law and human rights, data protection and ethical standards. Authorised persons also need to know how to apply effective decision models and tests to anchor their decision-making to accepted frameworks.

7.2 Police personnel should have completed a full programme of learning to ensure they are confident in understanding and applying their legal powers and can apply the relevant Decision Model for their force. This may require continuing professional development or refresher learning, especially when there is a change in job role. Those in roads traffic policing are likely to be comfortable as to how to access and apply driver licensing information. However, that access is now extended for use within wider policing and law enforcement powers and the range of authorised persons expanded for example to include civilian personnel who may not have undergone the same levels of training.

7.3. Purposes for which driver licensing information can be used

7.3.1 Section 71 of the Criminal Justice and Court Services Act 2000 (as amended by the Crime and Policing Act 2026) states that DVLA driving licence data may be used for policing and law enforcement purposes. Policing purposes[4] in England and Wales are defined as:

- protecting life and property
- preserving order
- preventing the commission of offences
- bringing offenders to justice
- any duty or responsibility of the police arising from common or statute law.

7.3.2 Policing Purposes in Scotland are set out in the Police and Fire Reform (Scotland) Act 2012[5]. The Act sets out a constable's general duties and overarching policing principles.

- to prevent and detect crime,
- to maintain order,
- to protect life and property,

[4] See paragraph 1.6 of the Code of Practice on Police Information and Records Management (PIRM).

[5] Police and Fire Reform (Scotland) Act 2012 https://www.legislation.gov.uk/asp/2012/8/contents

- to bring offenders with all due speed to justice
- to serve and execute a court warrant, citation or deliverance issued, or process duly endorsed

to attend court to give evidence.

7.3.4 Policing principles are further defined within the Police and Fire Reform (Scotland) Act 2012 thus

- improve the safety and well-being of persons, localities and communities in Scotland,

7.3.5 The Act goes on to say that policing should be:

- pursued in a way that is accessible to and engaged with local communities and promotes measures to prevent crime, harm and disorder and that,
- That the police service should be candid and be co-operative in proceedings including in all investigations.

7.3.6 Policing Purposes in Northern Ireland are outlined in Section 31A of the Police (Northern Ireland) Act 2000, requiring that police officers carry out their functions with the aim of securing the support of the local community, and of acting in co-operation with the local community. Section 32 provides a general duty of police officers to:

- protect life and property,
- preserve order,
- prevent the commission of offences,
- where an offence has been committed, to take measures to bring the offender to justice.

7.3.8 Law enforcement purposes are defined in section 31 of the Data Protection Act as:

> "The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

7.3.9 Data Protection is a reserved matter, so the definition applies across the UK. It will also apply in the Crown Dependencies and Gibraltar as the definition is taken from the EU Data Protection Directive, which has been adopted in all those jurisdictions.

7.3.10 For the avoidance of doubt the Code sees policing purposes as encompassing the common law policing duty regarding safeguarding which can be described as the protection of the health, wellbeing and human rights of individuals at risk, enabling them to live safely, free from abuse and neglect.

7.3.11 The legislation is explicitly designed to permit data obtained automatically from the DVLA to be used beyond road traffic purposes. This Code therefore particularly concerns this ability.

7.3.12 Authorised users should assure themselves that the use is necessary and proportionate. For example, it may be appropriate to find out whether someone under investigation relating to a situation where a person is likely to be driving. It may not be necessary to use the ability to check driving licences to identify a person stopped and searched particularly if there is no reason to arrest the person.

7.4. Access by policing oversight bodies

7.4.1 Four policing oversight bodies have been granted access to driver licensing information. These hold policing and law enforcement to account and may need such access to pursue an investigation into the conduct of policing and law enforcement activity. The bodies are:

i. Independent Office for Police Conduct
ii. Police Investigations and Review Commission
iii. Police Ombudsman for Northern Ireland
iv. Service Police Complaints Commissioner.

7.4.2 Authorised persons within those bodies will use driver licensing information within a distinct statutory and investigatory framework. In doing so, they should nevertheless be familiar with the concepts of policing purposes and law enforcement purposes and should apply the information only where its use is lawful, necessary and proportionate for the exercise of their functions.

7.5. Access to driver licensing information by direct application to the DVLA

The DVLA may be approached directly, on a case-by-case basis, with individual data enquiries. This will include cases in relation to medical details that are not available through the automated route. This might include details of medical conditions that might be materially useful when trying to locate a missing person. This might also include cases were further clarification on whether the information should be sought in the first instance, or how to interpret the information correctly.

Organisations listed in Section 71 of the 2000 Act which do not have automated access may contact the DVLA directly seeking disclosure of information.

7.6. Onward disclosure

7.6.1 The 2026 regulations set out how those accessing DVLA driver licensing data can onward share that data. Driving licence data may be onward shared within a single organisation if the future use relates

to the same purpose for which the data was obtained. An example would be transmission within an organisation to further investigate a person suspected of driving outside the terms of their licence. It may also be shared with those responsible for the prosecution of offenders or who deal with non-criminal penalties, for example driver education courses. A non-driving example might include a search to confirm the details of a person found injured as a result of a crime. The details might be forwarded inside the police force to facilitate victim support services.

7.6.2. Sharing with a partner organisation for the same purpose

It is also permissible to share driver licensing information to a partner organisation if it is being applied towards the same purpose for which it was obtained. This could include sharing with a body that is not eligible to access that information automatically. This must be linked to a shared event (investigation or operation). In the case of road traffic enforcement this might include passing details to courts for prosecution, or other organisations for driver education. Non-driving examples include where identification details need to be provided to a hospital, or to charities and organisations that can provide specialist help or assistance beyond the remit of the police.

7.6.3 Safeguarding disclosures

In matters of safeguarding officers and staff should take a pragmatic approach. If an organisation which has not been granted access has a concern about an individual's safety and well-being, they may apply to a policing body for assistance and should it be deemed necessary access to driver licensing information may be shared. For example, an ambulance service may approach a police control room for assistance in trying to locate the address of someone believed to have collapsed at home. A check on the drivers' register might provide the current address. Examples will also include police forces in different countries, who frequently contact UK police for assistance in identifying UK National who are in need.

7.6.4 What is not permissible

What is not permissible is an eligible organisation obtaining information on behalf of another that is not cited under Section 71 of the 2000 Act, where there is no joint endeavour or concern about an individual's safety. Anyone making such a request should be advised to contact DVLA. It is also not permissible for an eligible organisation to enter into an agreement with a non-eligible law enforcement partner to supply information upon request.

A number of use cases are provided in Appendix 3 to illustrate scenarios which might fall under these purposes and restrictions.

8. Promoting fairness

8.1. Legal and ethical obligations

Driver licensing information should not be used in a discriminatory or unethical manner. The ability to use driving licence data must be exercised in accordance with other legal obligations and duties, including the following:

- Data Protection Act 2018 ('the DPA')
- UK General Data Protection Regulation ('the UK GDPR')
- The Human Rights Act 1998, ensuring compliance with the European Convention on Human Rights ('the ECHR')
- The Equality Act 2010 or the equalities duties under the Northern Ireland Act 1998

8.2. The Data Protection Act 2018 and the UK General Data Protection Regulation

Driver licensing data held by the DVLA has not been collected for law enforcement purposes. Article 6 of the UK GDPR states that processing (and onward sharing is processing) shall be lawful only if and to the extent that one or more of a list of tests applies. In this case the processing is necessary for the performance of a task (preventing and detecting crime) carried out in the public. Once accessed for policing and law enforcement purposes it must also be managed according to the UK GDPR or Part 3 of the DPA 2018. In general, any processing must ensure that any information extracted is minimised, and that only the data that is needed for the purpose for which it is required is collected and retained.

8.3. Human rights, equality and ethics

8.3.1. The Human Rights Act 1998

The Human Rights Act 1998 gives effect in UK law to the rights set out in the ECHR. Section 6 of the Human Rights Act makes it unlawful for any public authority to act in a way which is incompatible with a Convention right. Article 8 of the ECHR sets out the right to respect for their private and family life, home, and correspondence. It provides that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society. This includes, among other things, where interference is necessary for the prevention of disorder or crime and for the protection of the rights and freedoms of others.

For the use of the data to be necessary and proportionate, the authorised person should be satisfied that the information sought is required to achieve the relevant purpose and that the purpose cannot be achieved by other less intrusive means. For the exercise of the power to be proportionate, they must consider if the purpose justifies the intrusion into the persons privacy, and that the amount of

information obtained has been minimised. For example, it may be proportionate to consider driving licence information for the investigation of serious crimes, but not for lower-level crime, such as anti-social behaviour or minor damage. However, there may be a local operation to target high incidences of damage to the properties of local shopkeepers causing repeated financial losses. Consider the circumstances that is being tested against the purpose.

8.3.2. Equality duties-

Under the Equality Act 2010 authorised persons must ensure they act in accordance with the Equality Act 2010 and the Public Sector Equality Duty (PSED) to eliminate discrimination, advance equality of opportunity and foster good relations between people when carrying out their duties. An Equality Impact Assessment (EIA) has been produced for legislative amendment that England, Scotland and Wales. This should be read by authorised persons. The Equality Impact Act 2010 does not apply in Northern Ireland. S75(1), and Schedule 9 of the Northern Ireland Act 1998 places a duty on public authorities to have due regard to the need to promote equality of opportunity between the nine protected equality categories. In Scotland the Equalities Act is enacted through The Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012.

8.3.3. Code of Ethics

The National Decision Model is underpinned by a Code of Ethics. The College of Policing sets out **the Code of Ethics** for England and Wales, there is also a specific **Code of Practice on Ethical Policing** for applies to the police forces maintained for the police areas of England and Wales **Code of Ethics for Policing in Scotland** sets out the standards of those who contribute to policing in Scotland and Police Service of Northern Ireland has its **Code of Ethics 2008**. Authorised persons should familiarise themselves with any Code of Ethics that may be relevant to their organisation.

9. Promoting accountability

9.1. Reporting

- The first level of accountability for this Code rests with the Home Secretary, through the Home Office. Section 71C of the Criminal Justice and Court Services Act 2000 (as amended) requires the publication of an annual report on the operation of the powers and the use of driver licensing information.
- The Annual Report should provide a clear and transparent account of how the powers have operated during the reporting period, including the extent to which access to DVLA data has supported policing, law enforcement and safeguarding purposes. It should cover both automated and manual access routes, explain the

broad categories of operational use, and show how compliance with this Code has been supported

- A core element of the Annual Report should be quantitative and qualitative information on usage. This should include high-level statistics showing how often driver licensing data has been accessed, for what types of policing or law enforcement purpose, and by which categories of authorised organisation. Alongside this, the Report should include illustrative case examples that demonstrate public benefit, such as protecting life, safeguarding vulnerable people, preventing serious crime or bringing offenders to justice. These examples should be anonymised and proportionate and should be used to evidence benefit realisation rather than to provide operational detail.
- The Annual Report should also address compliance, assurance and learning. It should summarise how monitoring and audit arrangements have operated across authorised organisations, highlighting themes emerging from audit activity rather than disclosing sensitive methodologies. Where misuse, error or unauthorised access has been identified, the Report should explain at a high level what occurred, how it was addressed, and what remedial or preventative action was taken. This section should also capture learning points, improvements to guidance or training, and any changes made to strengthen governance or controls.
- The Home Office has responsibility for overseeing the implementation of the Regulations and this Code of Practice, and for producing and publishing the Annual Report. In doing so, it must act as the central point of accountability to Parliament and the public, ensuring that information provided by authorised organisations is accurate, proportionate and consistent. The Home Office should set clear reporting requirements, including a standard data matrix, and work with partners to ensure that data is collected in a way that is manageable, comparable and focused on meaningful assurance rather than volume alone.
- In addition, the Home Office should use the Annual Report as a mechanism for continuous improvement. This includes reviewing trends, identifying emerging risks or areas of concern, and considering whether updates to guidance, training or the Code itself are required. The Home Office should also maintain ongoing engagement with policing bodies, oversight organisations and civil society, using feedback from the operation of the powers to ensure that access to driver licensing information remains lawful, necessary, proportionate and ethical, and continues to command public confidence.

9.2. Audit and monitoring

9.2.1. Distinction between monitoring and audit

Monitoring and audit serve related but distinct functions. Monitoring is an ongoing management activity, typically involving routine oversight,

management information and trend analysis to ensure compliance with expected standards. Audit, by contrast, is a more structured and independent process, conducted periodically or on a targeted basis, to test whether controls are effective and whether behaviour aligns with legal and ethical requirements. Monitoring may highlight areas of concern or emerging risk, which in turn can inform the focus of audit activity. Together, they form a complementary assurance framework, with monitoring providing continuous oversight and audit delivering deeper examination and challenge.

9.2.2. Purpose of audit

Audit is a formal mechanism for providing assurance that access to and use of driver licensing information is lawful, necessary, proportionate and ethical. It operates as a safeguard by examining how powers are exercised in practice, rather than how they are intended to be used. An effective audit function supports public confidence by demonstrating that access to DVLA data is subject to scrutiny, that misuse can be detected, and that appropriate action will be taken where standards are not met. Audit activity should be sufficiently robust to identify both systemic issues and individual misuse, while recognising the operational context in which policing and law enforcement decisions are taken.

9.2.3. Audit methods and escalation

Audit should be carried out through a combination of system-based checks, sampling of access records, and review of the recorded operational rationale for accessing driver licensing data. Auditors should be able to assess whether access was linked to a legitimate policing or law enforcement purpose and whether the decision-making was properly documented. Care should be taken not to publish or disclose detailed audit methodologies in a way that could enable evasion or misuse. Audit arrangements should also allow for escalation where inappropriate access is identified, including referral into disciplinary or professional standards processes where necessary, and for learning to be fed back into training and guidance.

9.2.4. Risk-based audit approach

Audit activity should be risk-based and proportionate, focusing attention where the potential for harm or misuse is greatest. Operational risk considerations may include known or emerging risks, such as inappropriate access driven by personal curiosity, including gender-based misuse of data, or the expansion of access in operational contexts such as stop and search where the necessity for DVLA data may not be clear. Forces may therefore choose to apply enhanced audit or additional supervisory checks in higher-risk contexts, for example where officers are working outside of active investigations, or where access patterns fall outside expected norms. A risk-based approach allows resources to be targeted effectively while reinforcing professional standards and ethical use of the data.

9.2.5. External scrutiny and oversight

This Code may be considered by those who hold policing to account—for example, the Independent Office for Police Conduct (IOPC). His Majesty's Inspectorate of Constabulary & Fire and Rescue Services (HMICFRS) will consider the Code in discharging its statutory responsibilities in respect of police forces in England and Wales, and similar arrangements are in place for forces in Scotland and Northern Ireland, by agreement.

10. Enabling performance

- Effective implementation of this Code depends on clear governance, training, supervision and assurance. Authorised organisations should ensure that the safeguards in this Code are supported in practice, so that access to driver licensing data is lawful, necessary, proportionate and capable of scrutiny.
- National training provider should support a consistent understanding of the extended powers. Local organisations remain responsible for ensuring that authorised persons are properly trained, that expectations are understood in practice, and that effective arrangements are in place to manage compliance.
- Responsibilities under this chapter operate at different levels: organisational, managerial, national auditor, training provider and individual. Together, these responsibilities should ensure that access is properly authorised, supervised, recorded and reviewed. Details of each level is covered in the Implementation of Code section.

10.1. Consultation

This Code has been subject to public consultation and there were recommendations for safeguards to be put in place to provide the public with reassurance that the extend power granted to policing and law enforcement is within clear legal and ethical boundaries. There is an ongoing process of consultation with civil society and bodies which hold policing to account to ensure that this Code is seen to be operating as an effective statutory safeguard.

11. Conclusion

- This Code of Practice provides a clear framework for the lawful, ethical and proportionate use of driver licensing information for policing, law enforcement and safeguarding purposes. It recognises the significant operational benefits that timely access to DVLA data can bring, particularly in protecting life, preventing crime and safeguarding vulnerable people, while making clear that such access carries responsibilities that must be exercised with care and professionalism.
- The Code places strong emphasis on accountability, transparency and assurance. Through clear expectations on governance, training, monitoring and audit, it establishes safeguards to ensure that access to driver licensing information is properly justified, recorded and capable of

scrutiny. These mechanisms are designed not to inhibit legitimate operational activity, but to reinforce good decision-making, deter misuse, and provide confidence that powers are being applied consistently with legal, human rights, data protection and ethical standards.

- By setting out responsibilities at organisational, managerial and individual levels, the Code supports a culture of ethical use and continuous learning across authorised organisations. It provides assurance to Parliament and the public that expanded access to driver licensing information is accompanied by robust oversight and effective controls, and that policing and law enforcement bodies remain committed to using these powers only where they are necessary, proportionate and in the public interest.

Appendix 1: Implementation of the Code

- The following implementation expectations are intended to support consistent application of the principles in this Code. They reflect the wider framework described in the draft Regulations, the record-keeping requirements in Appendix 3, the audit and monitoring model set out in this Code, and the current assumptions in policy, equality and data protection material that access will be role-based, trained, justified, auditable and capable of supporting annual reporting.
- Organisations are responsible for ensuring that their staff feel confident and supported in the use of DVLA data for genuine law enforcement and policing purposes. Even in a well-run regime there will be occasions where genuine mistakes are made, and the risk of a genuine mistake should not unduly inhibit access activity. Training should be provided that enables authorised officers to build up a model of acceptable use.
- Organisations should ensure that, in response to genuine errors, authorised officers are encouraged and supported to improve knowledge, skills and understanding so that better decisions are made in future. Rigorous audits should be in place to assist staff to identify areas for improvement as well as deliberate misuse.

1.1. What authorised organisations should have in place

1.1.1. Authorised organisations

- Authorised organisations should establish clear local accountability for compliance with this Code. That accountability should run from senior organisational leadership through Authorising Officers and operational managers to individual authorised users, so that responsibility for lawful access, proper supervision and corrective action is clear at all levels. Local governance should be capable of supporting national accountability, including the Home Office's annual reporting duty and the wider requirement to provide assurance to Parliament and the public.
- Organisations should also maintain effective governance, guidance, oversight, monitoring, audit and record-keeping arrangements to support lawful and ethical use, identify misuse or error, and ensure that any serious operational errors are investigated and addressed through appropriate remedial action.

- Authorised organisations should maintain a defined process for approving, recording and removing access. This should include verifying that any person granted access is properly authorised for their role, has completed the required training, holds the appropriate vetting clearance, and is recorded on an up-to-date local register of authorised users. Equivalent arrangements should exist for removing or suspending access where a person leaves a role, no longer requires access, transfers post, or becomes subject to disciplinary or criminal processes.
- Authorised organisations should ensure that local guidance is available and kept up to date on lawful use, necessity and proportionality, decision-making models, data minimisation, onward disclosure and professional standards. That guidance should make clear that the data is not to be used for personal interest, curiosity, convenience or speculative searching, and should explain the distinction between urgent operational use, routine automated access and cases that require direct engagement with DVLA, including where particularly sensitive medical information remains outside the routine automated route.
- Authorised organisations should ensure that each use of driver licensing data can be linked to a recorded policing or law enforcement purpose and an operational rationale. Records should be sufficient to show who accessed the data, what route was used, why the access was sought and, where relevant, whether onward disclosure took place. Organisations should ensure that their local systems, logs and governance arrangements are capable of supporting this requirement in a way that is attributable, reviewable and usable for audit and annual reporting.
- Authorised organisations should have routine monitoring and a structured audit capability. Monitoring should provide ongoing management oversight, trend analysis and exception reporting. Audit should provide a more formal and periodic test of whether controls are effective and whether access is lawful, necessary, proportionate and ethical. Audit should be risk-based and should be capable of identifying both individual misuse and wider organisational weaknesses, including patterns of access that suggest personal curiosity, weak justification recording, inappropriate onward disclosure or use in operational contexts where the necessity for DVLA data may be less clear.
- Authorised organisations should have clear rules and safeguards for onward disclosure. Those arrangements should ensure that onward sharing remains tied to the purpose for which the data was obtained, or to a properly connected purpose permitted by the Regulations, such as a shared investigation, criminal justice process or safeguarding activity. Local arrangements should make clear that organisations must not obtain or provide DVLA data on behalf of a body that is not eligible to access it where there is no joint endeavour or safeguarding need, and that onward disclosures should be limited, protected and recorded where required.
- Authorised organisations should also have arrangements to support organisational assurance and national reporting. This should include providing accurate and timely information on volumes and purposes of access, examples of operational benefit, themes from monitoring and audit, any sensitive or controversial uses, misuse or errors identified, and the remedial action taken. These arrangements should be proportionate

but robust enough to support the Home Office reporting data matrix and any future annual reporting requirement.

1.1.2. Managers

- Managers should ensure that staff who are able to access driver licensing data are appropriately authorised, vetted and trained before access is granted, and that they remain competent over time. Managers should ensure that staff have access to current guidance and understand the legal and ethical framework that governs use of the data, including lawful purpose, necessity and proportionality, data protection, human rights, equality considerations and professional standards.
- Managers should reinforce consistent use of recognised decision-making models and tests,and should expect staff to record their operational reasons clearly and accurately. Supervisory review should not be limited to technical entitlement management; it should also include review of whether access has been appropriate in practice, whether justifications are meaningful, whether onward disclosures have been handled correctly, and whether any refresher learning, corrective action or escalation is required.

1.1.3. Authorised users

- Authorised users should access driver licensing data only where there is a lawful and legitimate purpose connected to policing, law enforcement or safeguarding. They should satisfy themselves that access is necessary for that purpose, proportionate to the privacy intrusion involved, and limited to the information required. They should use recognised decision-making tools and tests,and should not use the data as a substitute for less intrusive options where those options are reasonably available and sufficient.
- Authorised users should record why the data was accessed, how it was used and, where relevant, how it was shared onward. They should follow local rules on confidentiality, handling, onward disclosure and secure retention, and should recognise that any extraction or inclusion of DVLA data within local records or case material brings with it normal organisational responsibilities for information management, review, retention and disposal. Authorised users should also maintain their knowledge and competence through refresher learning, updates to guidance and active continuing professional development.
- Authorised users should record why the data was accessed, how it was used and, where relevant, how it was shared onward. They should follow local rules on confidentiality, handling, onward disclosure and secure retention, and should recognise that any extraction or inclusion of DVLA data within local records or case material brings with it normal organisational responsibilities for information management, review, retention and disposal and should ensure that appropriate monitoring, audit, reporting and remedial action arrangements are in place, including for unauthorised access, serious errors and annual reporting requirements. Authorised users should also maintain their knowledge and competence through refresher learning, updates to guidance and active continuing professional development.

1.1.4. National auditor

- A national auditor, or equivalent national assurance body, should provide strategic assurance on how this Code is being implemented across authorised organisations. This should include oversight of the effectiveness of local audit arrangements, review of patterns and themes emerging from audit activity, and consideration of whether risks are being identified and managed consistently. National assurance should support comparability, learning and public confidence, while respecting operational sensitivities and avoiding publication of detailed methodologies that could facilitate evasion or misuse.
- National assurance should be capable of identifying systemic weaknesses, inconsistency between organisations, gaps in guidance or training, and emerging misuse risks. It should support improvement by highlighting lessons and good practice, and should be able to inform annual reporting, inspection or other national assurance activity. Where local audit functions exist, national oversight should also ensure that those local auditors are themselves operating appropriately and consistently.

1.1.5. Training provider

- A training provider should design, deliver and refresh learning and guidance for authorised users, managers and Authorising Officers. Training should reflect the law, the Code, operational decision-making models, necessity and proportionality, data protection, human rights, equality obligations, onward disclosure controls, and the consequences of misuse. Training should be capable of supporting both initial authorisation and refresher learning, including where access is extended to staff who may not previously have operated in road traffic policing contexts.
- Training material should be updated in response to changes in law, policy, operational practice, audit findings and lessons learned. It should help organisations evidence completion and consistency of learning, and should support continuing professional development rather than being treated as a one-off exercise. Where specialist functions exist, such as local auditors or those responsible for oversight, additional role-specific training should be available so that assurance activity is informed, consistent and effective.

Appendix 2: Reproduction of table in Section 71A(1)

Reproduction of table in Section 71A (1)

Person	**Authorising officer**
a constable	the person whose direction and control the constable is under
a member of civilian police staff	the person whose direction and control the member of civilian police staff is under
a police volunteer designated under section 38 of the Police Reform Act 2002	the chief officer of police whose direction and control the police volunteer is under
a National Crime Agency officer	the Director General of the National Crime Agency
a member, or a member of the staff, of the Independent Office of Police Conduct	the Director General of the Independent Office of Police Conduct
a member of the staff of the Police Investigations and Review Commissioner	the Police Investigations and 10 Review Commissioner
an officer of the Police Ombudsman for Northern Ireland	the Police Ombudsman for Northern Ireland
a member of a service police force or any other person who is under the direction and control of a Provost Marshal	the relevant Provost Marshal
a person appointed as an investigating officer by, or a member of the staff of, the Service Police Complaints Commissioner	the Service Police Complaints Commissioner
Isle of Man	
a member of the Isle of Man Constabulary, or an employee of the Isle of Man Public Services Commission	the Chief Constable of the Isle of Man Constabulary
an officer of customs and excise, or an immigration officer, of the Isle of Man	the Treasury Minister of the Isle of Man
a member of staff of the Financial Intelligence Unit of the Isle of Man	the Director of the Financial Intelligence Unit of the Isle of Man
Jersey	
a member of the States of Jersey Police Force	the Chief Officer of the States of Jersey Police Force
a deputy Agent of the Impôts, an officer of the Impôts, of the Bailiwick of Jersey	the Agent of the Impôts of the Bailiwick of Jersey
a member or employee of the Jersey Financial Intelligence Unit	the Director of the Jersey Financial Intelligence Unit
Person	**Authorising officer**

an employee of the Law Officers' Department	His Majesty's Attorney General for Jersey
Guernsey	
a member of the salaried police force of the Island of Guernsey a member or an employee of the States of Guernsey	the Chief Officer of the salaried police force of the Island of Guernsey,
an officer of customs and excise, or an immigration officer, of the Bailiwick of Guernsey	the Chief Officer of Customs and Excise of the Bailiwick of Guernsey
Guernsey a person authorised to exercise a function of the Director of the Economic and Financial Crime Bureau of the Bailiwick of Guernsey	the Director of the Economic and Financial Crime Bureau of the Bailiwick Guernsey
a member of staff of the Financial Intelligence Unit of the Bailiwick of Guernsey	the Head of the Financial Intelligence Unit of the Bailiwick of Guernsey
Gibraltar	
a member of the Royal Gibraltar Police	the Commissioner of the Royal Gibraltar Police
a member of the Gibraltar Defence Police	the Chief Officer of the Gibraltar Defence Police
a member of civilian staff in the Gibraltar Defence Police	the person whose direction and control the member of civilian staff is under

Appendix 3: Sample User Cases

The following scenarios are likely to be acceptable in all circumstances.

1. Road traffic stop – finding out whether the driver has a valid licence for the class of vehicle being driven.
2. Road traffic matter - finding out whether a person has a valid driving licence. Possible situations: organised misuse of the roads - intelligence is important to allow the police to decide what action to take prior to intercepting a vehicle.
3. Non-road traffic matter - finding out whether a person has a valid driving licence. Possible situations: persons transporting drugs by car - intelligence is important to allow the police to decide what action to take prior to intercepting that vehicle.
4. Safeguarding matter – road traffic accident identifying people injured.
5. Safeguarding matter – passing address information to a third party so that person can be safely transported home.

These examples may be appropriate in some circumstances, but only where access is necessary, proportionate and supported by a clear policing, law enforcement or safeguarding purpose. Driver licensing data must not be used for speculative searches or where less intrusive means is available.

The following scenarios may be appropriate in some circumstances:

6. Locating a relevant image in an investigation – obtaining the photograph of a registered keeper or insured person linked to a vehicle may be appropriate where no other suitable image is available.
7. Supporting an investigation at an address – where information indicates that named individuals may be resident at a property, checking whether a suitable image is available may be appropriate if this is necessary for the investigation and no less intrusive option exists.
8. Helping to locate a missing person – using the most recent available image may be appropriate where no suitable family-provided image is available, or where use of another image source may be inappropriate. This should not be read as changing existing procedures for missing person images.
9. Tracing witnesses or victims after a serious crime – access may be appropriate to help trace witnesses or victims who have provided names but not addresses, where other reasonable means are not available.

Access to and use of driver licensing data must be necessary, proportionate and supported by a clear policing, law enforcement or safeguarding purpose. It must not be used for speculative or unjustified searches, or where the purpose can reasonably be achieved by less intrusive means.

The following scenarios are unlikely to meet that threshold:

1. Stop and search, where no arrest has been made, solely to identify the individual.

2. Arrest, solely to identify the individual, unless there is reason to believe false details are being provided and this cannot reasonably be resolved by other available means, such as fingerprints.
3. Checking whether an authorised person is entitled to drive for employment or workforce management purposes, where a separate DVLA process exists for that purpose.

Access to Policing oversight bodies

We expect police oversight bodies access to DVLA data to focus on understanding what operational officers were able to see at a specific point in time. This will include what was accessed, and what information an officer would have been able to access should the DVLA database have been accessed.

Appendix 4: Requirements for Record Keeping

The authorising officer ("AO") must—

(a) be party, either directly or through an authorised representative, to a data sharing agreement with the Secretary of State in relation to their use of driver licensing information;

(b) ensure that every person AO authorises to receive driver licensing information ("relevant authorised person")—

(i) has completed appropriate training required by regulation 3(1)(a), and

(ii) holds the level of vetting clearance required by regulation 3(1)(b);

(c) ensure that every relevant authorised person undertakes appropriate refresher training at least [once a year] after they have become authorised persons;

(d) be able to provide appropriate training for every person it intends to authorise under section 71 of the Act and appropriate refresher training for all relevant authorised persons;

(e) ensure that every person who is responsible for the direction or control of an authorised person is made aware of—

(i) the requirements on AOs and authorised persons under these Regulations,

(ii) the ways in which driver licensing information is used in investigations in the United Kingdom or elsewhere, and

(iii) any developments in professional practice in relation to the use of driver licensing information;

(f) ensure that any unauthorised access to or use of driver licensing information is subject to disciplinary penalties, including, in a serious case, dismissal;

(g) prepare guidance for authorised persons on—

(i) the circumstances in which they may seek access to driver licensing information;

(ii) how they may obtain access to driver licensing information;

(iii) the purposes for which driver licensing information may be used, and to whom it may be disclosed;

(iv) the disciplinary penalties for inappropriate access to or use of driver licensing information;

(h) maintain a record of all relevant authorised persons;

(i) maintain a record of each time on which an authorised person has obtained driver licensing information, including—

i. the authorised officer making the request,

ii. the person to whom the information relates,

iii. the law enforcement or policing purposes and operational reasons for which access to that information was sought,

iv. whether the information was obtained by searching a DLI database, or by making a personal application for the information;

(j) monitor the use of driver licensing information by relevant authorised persons, including the persons to whom that information is disclosed.

Appendix 5: Onward Disclosure Scenarios

Always permitted

1. Onward sharing within one's organisation as part of the investigation for which the data was originally obtained. Officers and staff within one organisation should be able to share the data within their own organisation, whether this be for criminal justice purposes or as intelligence.
2. Onward sharing outside one's organisation as part of a joint operation conducted with another body not listed in Section 71 of the 2000 Act. Examples would be where the National Crime Agency is carrying out an investigation jointly with the Home Office concerning human trafficking. The NCA is able to access data, but the Home Office is not. We do not want the NCA having to remove DVLA driving licence data from intelligence it is sharing with the Home Office.
3. Onward sharing outside one's organisation as part of the criminal justice process, whether as used or unused material. We note that section 97A of the Road Traffic Offences Act 1988 provides a power for DVLA driving licence data to be shared with the courts and the police, but this only applies to courts in the UK and only applies with respect to motoring offences. We want to ensure that DVLA data obtained for other purposes may also be onwardly shared through the criminal justice process.
4. Further use within an organisation for a different law enforcement purpose, subject to necessity and proportionality and noting the need for the data to be current.

May be permitted.

5. Provision to another public body not listed in Section 71 of the 2000 Act to enable that body to assist in the welfare of a person. An example would be where the police wish to provide the ambulance service with a person's address so that the ambulance service has the fullest information available for it to carry out its work.

Unlikely to be permitted.

6. Provision to a body not listed in Section 71 of the 2000 Act for a purpose related only to the body not listed in Section 71.

The Legislative Framework (Regulation 5 of the Access to Driver Licensing Regulations 2026)

Disclosure of driver licensing information

(1) An authorised person may only disclose driver licensing information which has been made available for their use under section 71(1) of the Act in accordance with this regulation.

(2) Driver licensing information may be disclosed to—

(a) a person listed in column 1 of the following table, and

(b) for a purpose listed in column 2 of the entry for that person in the table.

Person/organisation to whom driver licensing information may be provided	**Purpose for which driver licensing information may be provided**
Any authorised person, or a volunteer acting under the direction of an authorised person	For a purpose ancillary to or connected with the use of the information by the authorised person by whom the information was first accessed
A member, or member of staff, of the Independent Office for Police Conduct ("IOPC")	For a function of the IOPC
A member of staff of the Police Investigations and Review Commission ("PIRC")	For a function of the PIRC
A member of the Police Ombudsman for Northern Ireland ("the Ombudsman")	For a function of the Ombudsman
A person appointed as an investigating officer by, or a member of staff of, the Service Police Complaints Commissioner ("the Commissioner")	For a function of the Commissioner
A member of— (a) His Majesty's Courts and Tribunal Service, (b) the Scottish Courts and Tribunal Service, (c) the Northern Ireland Courts and Tribunals Service, (d) the Gibraltar Courts Service, (e) the Military Court Service. (f) (Any court or tribunal— (i) of the Bailiwick of Guernsey, including any court or tribunal of Guernsey, Alderney or Sark; (ii of the Bailiwick of Jersey; (iii) in the Isle of Man (g) Any office-holder in Jersey, Guernsey or the Isle of Man having statutory responsibility for the administration of justice	For the administration of justice
A member of an organisation listed in Schedule 7 of the Data Protection Act 2018 or otherwise a competent authority by virtue of section 30(1)(b) of that Act	For a law enforcement purpose
A member of— (a) a regulated profession; (b) a registered charity; (c) an organisation with statutory obligations; (d) an organisation listed in Schedule 7 of the Data Protection Act 2018 (e) a competent authority	To assist the police with a policing purpose, where the police determine that this is required

within the meaning of section 30(1)(b) of the Data Protection Act 2018, which is not an organisation referred to in paragraph (d)	
A member of a body with functions outside the British Islands, the crown dependencies and Gibraltar which correspond to those of a police force in any part of the United Kingdom	to assist that body with a law enforcement purposes or policing purposes

(3) An authorised person may also disclose the name and licence number of a driver to UKROEd Limited to assist UKROEd Limited with the administration of speed awareness courses.

(4) In the table in paragraph (1)— “organisation with statutory responsibilities” includes any organisation which has such responsibilities under the law of the Bailiwick of Jersey, the Bailiwick of Guernsey, the Isle of Man or Gibraltar; “registered charity” means—

(a) in England and Wales, a charity registered under section 30(1) of the Charities Act 2011;
(b) in Scotland, a charity registered within the meaning of section 13(1) of the Charities and Trustee Investment (Scotland) Act 2005;
(c) in Northern Ireland, a charity registered under section 16(2) of the Charities Act (Northern Ireland) 2008; 4
(d) in Jersey, a charity registered under Article 8 of the Charities (Jersey) Law
2014(a);

(e) in Guernsey, a charity registered under Part III of the Charities etc. (Guernsey and Alderney) Ordinance 2021(b);

(f) in Isle of Man, a charity registered under Part 3 of the Charities Registration and Regulation Act 2019(c);

(g) in Gibraltar, a charity registered under the Charities Act 1962(d);

“regulated profession” has the meaning given in section 19 of the Professional Qualifications Act 2022(e);

“UKROEd Limited” or UK Road Offender Education, is a private not for profit company (registered number 08773977) responsible for the management and administration of the National Driver Offender Retraining Scheme on behalf of the Road Safety Trust (registered charity 1156300).

Schedule 1

Specific legislative provisions for Scotland

- The fundamental policing principles set out under the Police and Fire Reform (Scotland) Act 2012.
- The Equality Act 2010 (Specific Duties) (Scotland) Regulations 2012 places a responsibility on public authorities to assess and review all policies and practices to ensure that it complies with the equality duty in the exercise of its functions.
- The requirements under the Criminal Justice (Scotland) Act 2016 which make provision including police powers and the rights of suspects.
- The SBC code of practice – generally in terms of its guiding principles and ethical considerations for handling biometric data, the use of associated technologies and the overarching requirements to comply with DPA, ECHR, Equality legislation etc. This is a statutory Code brought into effect from November 2022 via regulations laid by the Scottish Ministers.
- The requirements under the Police (Ethics, Conduct and Scrutiny) (Scotland) Act 2025 which make provision including provision about a code of ethics and a duty of candour for the police; the vetting of constables and police staff; procedures for misconduct and the consequences of certain conduct by constables

More broadly there are relevant government outcomes/strategy docs (i.e. national performance framework and justice vision) but given the forthcoming Scottish election period, these are likely to become quickly out of date. It may be best to leave this for now and signpost any relevant ones produced by the new administration once these have been published.

Schedule 2

Specific legislative provisions for Northern Ireland

Schedule 3

Specific legislative provisions for Jersey

Schedule 4

Specific legislative provisions for Guernsey

Schedule 5

Specific legislative provisions for Isle of Man

Schedule 6

Specific legislative provisions for Gibraltar

Schedule 7

Data that is available to police and law enforcement agencies via automated means

Name and description	
Driving Licence Number	The full Driving Licence Number including the check digits.
First name(s)	Driver's given name(s).
Last Name	The driver's surname or family name
Title	Title in full mode of address, e.g. Mr, Miss, Lord.
Name format	Instructions for formatting of the full mode of address from names and titles, e.g. With Title.
Full mode of address	Fully formatted name of an individual including salutation.
Gender	Gender of the driver, e.g. "Male", "Female".
Date of birth	Format YYYY-MM-DD.
Place of birth	The place in which the driver was born.
Photograph	The photograph DVLA holds on an individual.
Death Notification Date	Date DVLA were notified that a driver is deceased (record will skeletonize after 3 months).
Address	Address details.
Current Driving Licence Number	The full Driving Licence Number including the check digits of the current driver record if this is a cross referenced record.
Eyesight	Eyesight standard or requirements.
Hearing	Hearing standard or requirements.
Is Military	Indicates if driver is a military driver.
Disqualified until	Format YYYY-MM-DD.
Disqualified for Life	Indicates if a driver is disqualified for life.
Disqualified Pending Sentence	Indicates if a driver is disqualified pending sentence.
Approved Driving Instructor	Indicates that the driver is an approved driving instructor by DVSA.
Retained C1 D1 Entitlement	Indicates that the higher categories C1 and D1 have been retained when over 70 or have been medically revoked.
Photo Valid From Date	Date when image becomes valid (YYYY-MM-DD).
Photo Valid To Date	Date when image expires (YYYY-MM-DD).
Driver redirect (not held in datastore but returned to end user where x-ref driver number enquired upon)	Indicates if record was redirected to a cross reference record.
Driver Signature	The image of the signature DVLA holds for an individual.
Previous driving licence	
Previous Driving Licence Number	Driver number previously assigned to this driver.
Previous First Name(s)	Forenames used on the previous driving licence.
Previous Last Name	Last names used on the previous driving licence.
Previous Date of Birth	Calculated DOB of previous driving licence.

Licence data	
Licence type	Whether the licence is “Provisional” or “Full”.
Licence Status	The current activation state of the licence, e.g. “Valid”, “Revoked”, “Expired”.
Status Qualifier	Information or restrictions relating to a Licence Status, e.g. “Until test passed”, “For re-assessment only”, “Pending sentence”.
Country to which Exchanged	The country to which this licence was exchanged.
Entitlements (under current legislation)	
Entitlements	Array of entitlement objects*
Category Code	Licence category code.
Category Legal Literal	Category literal.
Category Short Literal	Category short description.
Category Type	Full or Provisional entitlement for the category.
From Date	The first date on which the category becomes valid (YYYY-MM-DD).
Expiry Date	The last date on which the category is valid (YYYY-MM-DD).
Restrictions	Restriction codes and literal that apply to the category**
Restricted to Automatic Transmission	Whether the category is restricted to automatic transmission only.
Category Status	The status of the category, e.g. Valid, Revoked, Suspended.
From Non-GB	Indicates if the category was assigned based on the entitlement from a non-GB licence during exchange.
Restriction data items	
Restriction Code	Restrictions that apply to a category.
Restriction Literal	Based on restriction code.
Test Pass Data	
Test Pass	Array of test pass objects*
Test Pass Data Items	
Type	The type of test passed, e.g. Driving Licence.
Category Code	Category in which the test was passed.
Category Short Literal	A short, easily consumed literal of an entitlement category (Entitlement category code).
Category Legal Literal	Full legal description of an entitlement category.
Test Date	Date on which the test was passed (YYYY-MM-DD).
Status	Whether the test pass has been claimed, cancelled, or remains unclaimed.
With Automatic Transmission	Denotes if the test was in an automatic transmission vehicle only.
Vehicle Adaptations	Any adaptations that were in use during the test. These are restriction codes.
With Trailer	If a trailer was attached during the test.
Extended Test	If the test was extended, such as following a DTETP.

Licence Surrendered	If the previous licence was surrendered following the test.
Testing Authority	Who performed the test, e.g. DVSA, MOD.
Token	
Type	Type of token produced (paper/plastic).
Driving Licence Number	Driving licence number.
Issue Number	Issue number as displayed on licence.
Valid from Date	Date from which the token is valid (YYYY-MM-DD).
Valid to Date	Date to which the token is valid (YYYY-MM-DD).
Is Provisional	Denotes provisional only entitlements.
Entitlements Data (as presented in TOKEN)	
Entitlements	Array of Entitlement Objects*
Category	Licence category code.
Category Legal Literal	Entitlement category code.
Category Short Literal	Entitlement category code.
Category Type	Full or Provisional entitlement for the category.
Category from Date	Start of the category entitlement period (YYYY-MM-DD).
Category Expiry Date	Expiry of the category entitlement period (YYYY-MM-DD).
Category Restrictions	Array of Category Restriction Objects**
Group	Pre-harmonisation group code.
Group Legal Literal	Entitlement group code.
Group Short Literal	Entitlement group code.
Group Type	Full or Provisional entitlement for the group.
Group from date	Start of the group entitlement period (YYYY-MM-DD).
Group expiry date	Expiry of the group entitlement period (YYYY-MM-DD).
Group Restrictions	Array of Group Restriction Objects***
Category Restrictions Data	
Category Restriction Code	Restrictions that apply to a category.
Category Restriction Literal	Created from static data based on restriction code****
Group Restriction Data	
Group Restriction Code	Restrictions that apply to a category.
Group Restriction Literal	Created from static data based on restriction code****
Endorsements Data	
Detailed Endorsements	Array of detailed endorsement objects*
Appeal Court Code	Code of the court at which the appeal was registered.
Appeal Date	Date on which the appeal to the conviction was made.
Conviction Date	Date on which the court hearing was held.
Conviction Court Code	Identifying code of the legal court where the conviction produced the endorsement.
Disqualification	Disqualification object**
Disqualification Suspended Pending Appeal Date	Date on which disqualification started with an appeal pending.

Disqualification Re-imposed Date	Date on which the disqualification was re-imposed.
Disqualification Removal Date	Date on which the disqualification was removed pending appeal.
Disqualified Pending Sentence	Type of disqualification imposed pending sentencing.
Expiry Date	The last date on which the endorsement applied, i.e. the endorsement has expired and is not applicable after this date.
Fine	The financial penalty applied to the endorsement.
From Date	Start date from which the endorsement applies.
Identifier	The unique identifier supplied by the issuing authority such as the court, or a generated unique ID.
Markers	Markers that apply to the endorsement, i.e. hardship claimed***
Next Report Date	When the next report is due.
Notification Source	Who notified the endorsement to DVLA (court code).
Offence Code	The code of the offence causing the endorsement.
Offence Legal Literal	Full legal description of an endorsed offence.
Offence Date	Date on which the endorsed offence occurred.
Other Sentence	Non-financial, non-custodial sentence type.
Other Sentence Literal	Will provide the meaning of the code.
Penalty Points	The number of penalty points given.
Prison Sentence Suspended Period	Details relating to suspended sentencing*****
Rehabilitation Course Completed	Indicates a rehabilitation course was undertaken to reduce sentence.
Sentence Date	Date on which the sentence was issued.
Sentencing Court Code	The court that issued the sentence.
Disqualification Data	
Type	Extended disqualification, e.g. DTTP, DTETP, RTTP.
For Life	Is disqualified for life.
Years	Number of years on the disqualification.
Months	Number of months on the disqualification.
Days	Number of days on the disqualification.
Declared Hardship	Indicates hardship was claimed in the court case, thereby avoiding a disqualification.
Years	Number of years of sentence that is suspended.
Months	Number of months of sentence that is suspended.
Days	Number of days of sentence that is suspended.
Hours	Number of hours of sentence that is suspended.