HAMBLETON
DISTRICT COUNCIL

Appropriate Policy Document

Law Enforcement Processing

a place to *grow*

Contents

Author:	Veritau DPO
Management Team:	May 2021
Version:	1
Policy approved date:	TBC
Policy reviewed:	N/A
Policy updated/amended:	N/A
Policy review date:	TBC

Update and approval

This Policy shall be updated annually or, if deemed necessary, whenever there is a need or requirement to do so. It will be updated in respect of changes within the privacy field, other regulatory changes, changes in the market where the District Council operates and internal changes within the District Council. Any changes to this Policy are subject to approval by the SIRO.

1. Introduction

In May 2018 the UK's existing Data Protection Act was replaced by the EU's General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). Whilst the GDPR (now the UK-GDPR since the UK left Europe) runs in conjunction with the DPA, the EU's Law Enforcement Directive (LED) was fully incorporated into the DPA and became Part 3 of the Act.

The council has now created this policy in compliance with section 42 of the DPA to cover data processed under Part 3 of the Act alone. It is important to note that the UK GDPR **does not apply** to this type of processing of personal information.

2. Scope

The Information Governance Strategy and corresponding policies apply to all Hambleton District council officers, any authorised agents working on behalf of the council, including temporary or agency staff, elected members, and third party contractors. Individuals who are found to knowingly or recklessly infringe this policy may face disciplinary action.

3. Purpose

This policy explains the council's procedure for securing compliance with the data protection principles listed below in relation to sensitive processing for law enforcement purposes. The policy also explains the retention and erasure policies in relation to the sensitive processing.

This document demonstrates that the processing by the council of personal data falling into the category of "sensitive processing", is compliant with the data protection principles set out in Part 3 of the DPA.

The DPA 2018 includes the requirement for an Appropriate Policy Document (APD) to be in place when processing such data under certain specified conditions. This document incorporates the council's APD. The information supplements the council's privacy notices.

The council carries out sensitive processing for a number of different law enforcement purposes but does not need a separate policy document for each condition or processing activity, and this document covers them all. It references policies and procedures which are relevant to all the identified processing. Therefore it explains the council's compliance with the principles in general terms.

As the council relies on the conditions identified below, this policy should be considered as a part of the general record of processing activities under section 61 of the DPA. Other information in that record is to be found within the council's Information Asset Registers. This document should therefore be read in conjunction with them.

4. Definitions and description of data processed

Part 3 of the DPA is concerned with the processing of Criminal Offence (CO) data by a competent authority. An organisation can only be a "competent authority" if the organisation/body is specifically mentioned in Schedule 7 of the DPA (Local Authorites are not included here) or, 'any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes'

"Law enforcement purposes" is defined in section 31 DPA 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 in public security'.

The council, therefore, will be a competent authority for the processing of some CO data, but not others. For example, the council will be a competent authority for the processing relating to some environmental offences, as it holds statutory powers to enforce criminal law. Where however, a council needs to share information with a Police force to aid them with their investigation, a council will not be a competent authority and would instead be processing information under GPDR as per Schedule 2, Part 1(2) - Crime and taxation: general.

"Sensitive processing" is defined in Section 35(8) of the DPA as the processing any of the below by a competent authority for a law enforcement purpose:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation
- Biometric data for the purpose of identifying individuals

5. The data protection principles

The principles set out in Part 3 of the DPA require personal data to be:

1. Processed lawfully and fairly **(lawfulness and fairness)**.
2. Collected for specified, explicit and legitimate law enforcement purposes, and not further processed in a way which is incompatible with those purposes **(purpose limitation)**.
3. Adequate, relevant and not excessive in relation to the purposes for which it is processed **(data minimisation)**.
4. Accurate and where necessary kept up to date **(accuracy)**.
5. Kept for no longer than is necessary for the purposes for which it is processed **(storage limitation)**.
6. Processed in a way that ensures appropriate security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage **(integrity and confidentiality)**.

In addition the council is also responsible for demonstrating compliance with the above principles (accountability principle).

Accountability Principle

The Council has put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer, Veritau Ltd, which reports directly to the Council's highest management level.
- Taking a 'data protection by design and default' approach to its activities including the use of data protection impact assessments (DPIAs).
- Maintaining documentation of its processing activities through Information Asset Registers.
- Adopting and implementing data protection policies and ensuring it has written contracts in place with its data processors.
- Implementing appropriate security measures in relation to the personal data it processes.
- Carrying out DPIAs for its high risk processing.

The Council regularly reviews its accountability measures and updates or amends them when required.

Principle 1: lawful and fair

Processing personal data for law enforcement purposes must be lawful and fair. Processing will not take place unless the reason to do so derived from legal powers granted to the Council.

The Council provides clear information about why it processes personal data in its privacy notices and this policy document.

Where consent is requested from an individual to allow sensitive processing, the individual will be provided with full details of what will happen to their data and the length of time it will be retained. The individual will also be advised of their right to withdraw their consent.

If the law enforcement purpose would be prejudiced by notifying the subject of the processing of their data then an exemption from the above obligations may apply.

Where sensitive data is being processed, the Council will ensure that it meets one of the conditions within Schedule 8 and continues to ensure that an appropriate policy document (this policy) is in place.

Principle 2: purpose limitation

Personal data collected for a law enforcement purpose must be specified, explicit and legitimate.

Personal data can be processed for a further purpose, but no further processing can be carried out that is incompatible with the initial processing purpose. To be compliant with this principle the Council must be authorised by law (i.e have powers to enforce the criminal law) to process for the further purpose, and the processing must be necessary and proportionate to that purpose. For example, information collected for the purpose of an environmental offence investigation must not be used for the incompatible purpose of sending further unrelated communications.

Principle 3: data minimisation

The Council collects personal data necessary for the relevant law enforcement purposes and ensures it is not excessive. The information it processes is necessary for and proportionate to its purposes. Where personal data is provided to the Council or obtained by it, but is not relevant to its stated purposes, it is to be erased.

Principle 4: accuracy

The Council will ensure that as far as possible the data they hold is accurate and is kept up to date. In some instances, the factually inaccurate information may need to be retained such as in a statement from a witness. Where the Council becomes aware that personal data is inaccurate or out of date it will take every reasonable step to ensure that data is erased or rectified without delay. Where this is not possible, an addendum will be added advising of the inaccuracy. Further to this, where necessary, the processing will be restricted in accordance with sections 46 and 48 DPA. If inaccurate data has been disclosed, the recipient will be advised of this as soon as practicable.

The Council will look to ensure that there is a distinction between data to the below categories of individuals:

- Suspects
- Those convicted of criminal offences
- Victims
- Witnesses or those with information about offences

The Council will, as far as possible, ensure that personal data based on personal assessment and opinion (including intelligence) is distinguished from that which is based on fact.

Principle 5: storage limitation

Personal data will not be kept for longer than necessary for the law enforcement purpose. Retention periods are defined within the Council's Retention Schedule.

Once this retention period has been reached, data will be deleted unless it is being kept longer for archiving purposes.

The Council's retention schedule is reviewed from time to time and updated when necessary.

Principle 6: integrity and confidentiality (security)

Electronic information is processed within the Council's secure network. Hard copy information is processed in line with its security procedures.

The Council's electronic systems and physical storage have appropriate access controls applied.

The systems the Council uses to process personal data allow it to erase or update personal data at any point in time where appropriate.

6. Schedule 8 conditions for processing

Further conditions for processing sensitive data for a law enforcement purpose are created by Schedule 8 of the DPA. The most relevant to a local authority are:

- **Paragraph 1** Statutory, etc purposes
- **Paragraph 4** Safeguarding of children and of individuals at risk
- **Paragraph 5** Personal data already in the public domain
- **Paragraph 6** Legal claims
- **Paragraph 8** Preventing fraud
- **Paragraph 9** Archiving

7. Retention and erasure

The council's retention and erasure policies are based on the purpose for which records are created and used. They do not identify categories of data and therefore do not explicitly state how long any of the special categories of data will be retained. There is no retention period specific to any of the special categories. Data falling into any of the special categories will be retained according to its purpose, not its category.

However the Information Asset Registers do identify what council data is included in each asset, and indicate how long it will be retained. The assets relate to all of the council's services, including its internal management.

The Retention Policy sets out retention periods for the types of records that the council uses to provide all of those services and internal management.

8. Contact

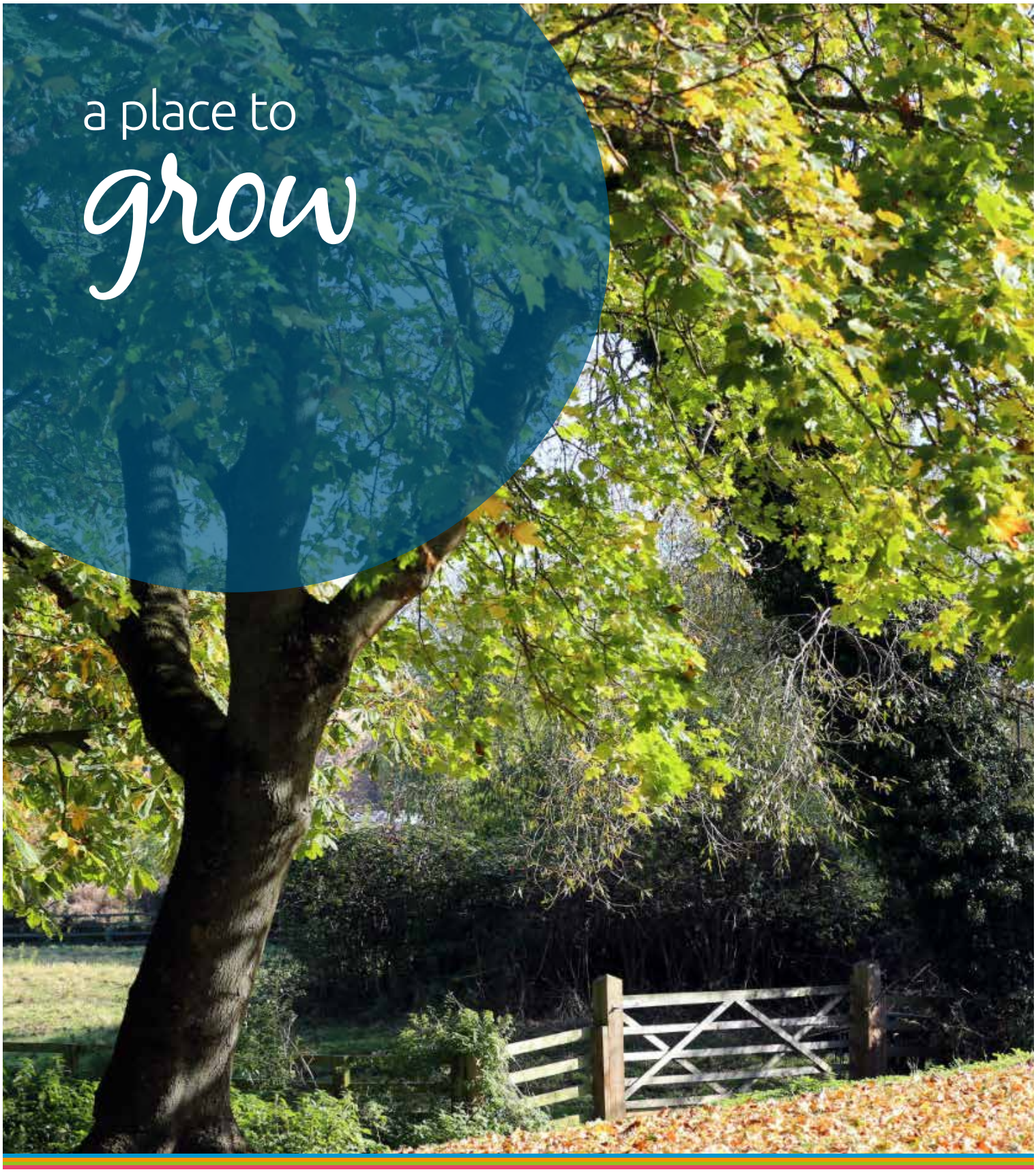
Senior Information Risk Owner (SIRO)
Dr Justin Ives
Chief Executive
Justin.Ives@hambleton.gov.uk

Specific Point of Contact (SPOC)
Gary Nelson
Director of Law and Governance (Monitoring Officer)
Gary.Nelson@hambleton.gov.uk

Data Protection Officer (DPO)
Information Governance Team
Veritau Limited
infogov.HambletonDC@veritau.co.uk


HAMBLETON
TRICT COUNCIL


HAMBLETON
STRICT COUNCIL



HAMBLETON
DISTRICT COUNCIL

Civic Centre, Stone Cross, Rotary Way, Northallerton, North Yorkshire DL6 2UU
01609 779977
hambleton.gov.uk

This information is available in alternative formats and languages