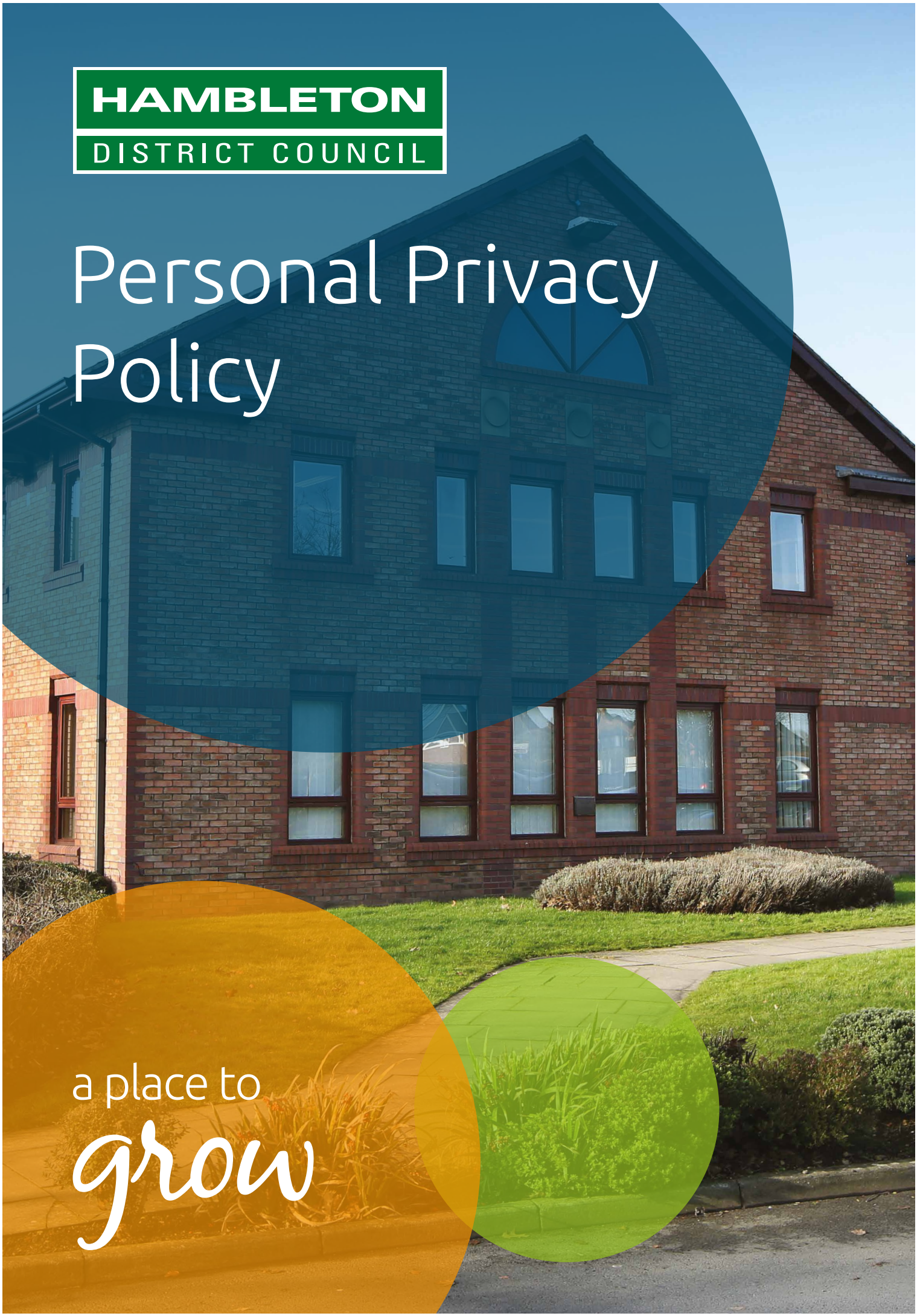
HAMBLETON
DISTRICT COUNCIL

Personal Privacy Policy



a place to *grow*

Contents

Version:	1.0
Publication date:	3.10.19
Policy review date:	3.10.20

Introduction and scope

In May 2018 the UK's existing data protection framework was replaced by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. As part of Hambleton District Council's compliance with this new legislative framework it has introduced a new information governance policy framework.

The Personal Privacy Policy sets out how the council will inform Data Subjects about how and why the council uses their data, what measures the council has in place to ensure data disclosures are lawful and secure, and how the council addresses risks to the data protection rights and freedoms of individuals. The Policy is concerned with, in particular, the first, second, and sixth data protection Principles:

Article 5(1)(a) Personal data should be processed lawfully, fairly, and in a transparent manner in relation to the data subject

Article 5(1)(b) Personal data should be collected for specified, explicit, and legitimate purposes...

Article 5(1)(f) Personal data should be processed in a manner that ensures appropriate security of the personal data

Who does this policy apply to?

The Information Governance Strategy and corresponding policies apply to all 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.

What does this policy apply to?

The Information Governance Strategy and corresponding policies apply to information in all forms including, but not limited to:

- hard copy or documents printed or written on paper
- information or data stored electronically, including scanned images
- communications sent by post/courier or using electronic means such as email, fax or electronic file transfer
- information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card
- information stored on portable computing devices including mobile phones, tablets, cameras and laptops
- speech, voice recordings and verbal communications, including voicemail
- published web content, for example intranet and internet
- photographs and other digital images.

Privacy notices and consent forms

The GDPR states that when a Data Controller is collecting personal data from a Data Subject it must provide that Data Subject with specified information about the nature of the intended processing. Likewise, if the Data Controller is processing personal data, about a Data Subject, that has been obtained from another source then it must make available, to the Data Subject, specified information about the nature of the processing.

In both cases the council must communicate the specified information, to the data subject, prior to collection or as soon as possible thereafter.

Due to the council's large and varied work it has opted to adopt a three tier privacy notice system in order to fulfil this requirement. The three tiers being: a corporate privacy notice, a series of service specific privacy notices, and the utilisation of concise 'just in time notices'. This is an approach recommended in the transparency code of practice issued by the Information Commissioner's Office (ICO).

These notices will be easily accessible, written in plain English, and will include a glossary of Data Protection terminology so that all council service users are able to understand how the council uses their data.

Corporate Privacy Notice

The council will maintain and publish a Corporate Privacy Notice on its website. The Corporate Notice will be set out in a Questions and Answers format as suggested by the transparency Code.

The Corporate Notice will state:

- what the council is and who the council's Data Protection Officer is,
- the high-level reasons for requiring personal data,
- a high-level overview of who has access to personal data (internally and externally) - for example the Police or Anti-Fraud agencies.
- an overview of the council's Information Security arrangements,
- the council's high level lawful basis for data processing and the council's high level data retention policy,
- whether the council stores any personal data outside of the EU,
- what an individual's rights are over their personal data,
- how they can complain about how the council uses their personal data.

The Corporate Notice will be reviewed and updated by the council's Data Protection Officer on an annual basis or otherwise when required by legislative or regulatory updates.

Service Specific Privacy Notices

The council will also maintain and publish Service Specific Privacy Notices for each instance of processing. These notices will be published alongside the Corporate Notice with the intention that individuals read both notices to achieve a complete understanding of how the council processes personal data.

These notices will state:

- who the Data Controller is and who the Data Protection Officer is
- what personal data the service processes and the purpose of processing
- who has routine access to the Personal Data
- retention periods of the Data
- the lawful basis for processing.

All Service Specific Notices will contain a link to the Corporate Notice and will be set out in a Questions and Answers format as suggested by the transparency Code.

Each Service area is responsible for ensuring their Privacy Notice is up to date and readily available. The Data Protection Officer will be responsible for providing a Privacy Notice template, approving all notices, and maintaining a log of notices so that these can be reviewed periodically.

'Just in Time' Notices

Just in time notices are to be included on all electronic and paper data collection forms issued by the council. These should state the purpose of collection and where service users can go to find out more information about their Privacy. For example:

> The council is collecting your personal data for the purpose of XX. For more information about how and why the council uses your data, including your data protection rights, visit **hambleton.gov.uk/privacy**

It is the responsibility of each service area to ensure these notices are utilised.

Consent Forms

As well as having a robust and extensive set of Privacy Notices the council must also ensure that its Consent Forms are updated and lawful. The GDPR states that when a Data Controller is relying on consent as a lawful basis then the Data Controller has an obligation to provide the Data Subject with a clear statement regarding what the Data Subject is consenting to. Furthermore, the council must be able to demonstrate consent preferences upon request.

When relying on consent the council will ensure that a consent form is issued to the Data Subject. This consent form must:

- state specifically what the Data Subject is being asked to consent to
- state where the Data Subject can find out more information about the processing of their Personal Data (i.e. link to Privacy Notice)
- state how long the consent preferences are valid for (including whether consent is valid until preferences are changed by data subject)
- state that the Data Subject can change their consent preferences at any time and provide instructions as to how they can do this

- include a 'Yes' or 'No' consent tick box
- include a signature and date box.

Each Service area is responsible for ensuring consent forms are utilised each time the council relies on consent as a lawful basis for Data Processing. Each Service area is also responsible for keeping track of consent preferences and keeping the evidence required to demonstrate consent preferences.

Where possible consent should be given in writing. It is accepted that in some specific situations this will not be possible and the council will have to rely on oral consent. In these circumstances the officer should ensure that this is documented and confirmation sent to the applicant in order to verify their consent preferences.

Information sharing

In order to optimise the facilities that it provides to service users the council appreciates the benefits that information sharing with Partner organisations brings. The council also appreciates that information sharing is not without risk. Therefore, the council will implement measures and safeguards to ensure Information Sharing is conducted lawfully, transparently, and securely.

The process of Information Sharing can be separated into two types of disclosures: routine data disclosures and ad-hoc data disclosures.

Routine Data Disclosures

Where the council routinely discloses personal data to other data controllers, including boards, multi-agency teams, and working together partnerships, an Information Sharing Agreement must be established.

These agreements must detail the lawful basis for processing, how the controllers will comply with the data protection principles, and how the controllers will uphold data protection rights.

Service Areas are responsible for identifying when an agreement is required and are responsible for organising and writing such an agreement. The relevant Information Asset Owner must sign all Information Sharing Agreements in their service area. If the agreement is considered to be high risk then the council's Data Protection Officer should sign the agreement. Where high risks can not be mitigated or where the risks could be considered contentious then the Senior Information Risk Owner (SIRO) may be required to sign the agreement too.

Information sharing arrangements between most North Yorkshire public-sector organisations must use the Information Sharing template(s) stipulated by the Multi-Agency Information Sharing Protocol (see below). The Data Protection Officer will provide a template agreement for arrangements with organisations who are not a signatory to the Protocol.

Ad-Hoc Data Disclosures

As well as routine information disclosures, the council will often be required to disclose information to another data controller on an ad-hoc basis. This could be, but not necessarily limited to, to fulfil a legal requirement, for crime prevention and/or detection, or for regulatory purposes.

Where possible, all requests for personal data should be submitted in writing by the requesting data controller. This should state:

- the name and address of the data controller
- their purpose and lawful basis for processing the personal data
- whether the council is able to tell the data subject of disclosure
- how not disclosing the information would prejudice their purpose
- a counter signature of a senior officer.

When received it is the responsibility of the Service Area to decide if disclosure is appropriate and subsequently arrange for the data to be disclosed. The Service Area may decide to apply limitations to the disclosure.

The Data Protection Officer does not need to be informed of all Ad-Hoc data disclosures but can offer the service area advice and assistance in deciding whether disclosure is appropriate.

Where it is not possible for a request to be made in writing, due to the disclosure being made as part of an emergency situation, then the disclosing officer will gather authorisation from their manager and must obtain a retrospective application which details the above criteria.

Records of Ad-Hoc data disclosure should be kept on the file of the Data Subject so that, if the data subject submits a Subject Access Request, the council is able to easily identify which other organisations have had access to their personal data.

Multi-Agency Information Sharing Protocol

The council is a member and signatory to the North Yorkshire Overarching Multi-Agency Information Sharing Protocol (MAISP). This Protocol sets out the standards and procedures for information sharing between signatory organisations.

Officers who are routinely involved in data disclosures, or are organising a routine information sharing agreement, should ensure they operate within the Protocol's guidelines.

The Data Protection Officer is responsible for representing the council at the Protocol's operational meetings.

Data processors

The council will often employ contractors to carry out data processing activities. These contractors are known as 'Data Processors'. Examples of Data Processors include:

- a software provider who hosts a database for the council
- a translation or clerking service
- a charity who works with individuals on behalf of the council.

Council employees, elected members, or in-house support service are not data processors.

All third party contractors who process data on behalf of the council must be able to provide assurances that they have adequate data protection controls in place to ensure that data that they process is secure.

The council's standard terms and conditions will include data processor clauses. A list of mandatory terms and details can be found in Appendix One of this Policy.

The SIRO may insist that any data processing, by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place.

If any data processing is going to take place outside of the UK then the Data Protection Officer must be consulted prior to any contracts being agreed.

Records of Data Processors

The council is not obliged to routinely inform data subjects of which Data Processors it employs. However, the council must inform data subjects about the categories of data recipients and as such a paragraph about the use of Data Processors will be included on the council's corporate privacy notice.

The council will keep a record of which data processors have access to personal data within the council. This will be done through the council's corporate information asset register (IAR). The IAR is governed by the council's 'Information Management Policy'.

Data Protection Impact Assessments (DPIA)

The council will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR. This assessment will consider the privacy risks and implications of new projects as well as providing mitigating solutions to the identified data protection and privacy risks.

The IAO is responsible for ensuring the completion of the DPIA. The DPO must advise on such assessments.

High risk data processing projects where it is not possible to mitigate the risks to an acceptable level may require authorisation from the Information Commissioner's Office. The DPO will advise where this is the case and will liaise with the ICO, following consultation with the SIRO. The DPO will keep a register of completed assessments and ensure that officers have access to a current assessment template.

Training

The council will provide basic training to all council officers and elected members so that every council employee is aware of the council's responsibilities under Freedom of Information Act 2000, Environmental Information Regulations 2004, and Data Protection Act 2018. This includes all temporary staff and volunteers.

Training will be undertaken PRIOR to any individual being given access to council systems or personal information. Advanced training will be given to officers who are expected to collate requested information and respond to requests for information.

Information governance training will be renewed annually for officers, and each time they are elected for elected members.

The council will also ensure that third party contractors ensure their staff are adequately trained in information governance.

The SIRO is responsible for ensuring the training resources are effective and training requirements are adhered to.

Automated decision making technology

When the council utilises Automated Decision Making Technology it is obliged to ensure that it maintains sufficient safeguards to protect the rights and freedoms of data subjects.

The council's 'Data Protection Rights' Policy details how the council will deal with a Data Subject's rights to be informed of, and object to, Automated Decision Making Technology.

Definition and Scope of Automated Decision Making Technology

The Information Commissioner's Office defines Automated Decision Making as using automated algorithmic technology to make predictions or decisions about an individual based on data about their personality, behaviour, interests, or habits.

This policy does not apply to automated analysis processing where aggregated data is being used for research, to generate statistics, or to direct council policy.

The policy also does not apply to processing where automated technology has been used for a calculation but there has been human review before a decision is made i.e. an assessment tool.

Data Integrity and Algorithmic Integrity

In order to ensure that decisions are being made fairly, and in accordance with the Data Protection Principles, the council must ensure that the data being input is up to date and accurate. Where possible the council will allow Data Subjects to input their own data. Where this is done the data field descriptions must be clear, concise, and must not be misleading.

Where council officers are inputting personal data from other existing records they must carry out and record checks to ensure that the data is correct, up to date, and relevant for the purposes of processing. Officers must also ensure there are no legal restrictions to the use of automated decision making. Where possible, any legal restrictions will be noted on the Data Subject's main file.

Likewise when using algorithmic technology, the council must be able to guarantee the quality of the algorithm and must be able to understand the algorithmic calculation should an appeal be lodged by the Data Subject. Algorithmic technology must be procured, with proper procurement checks taking place, before being utilised.

Data Risks

Council officers must complete a Data Protection Impact Assessment prior to the use of Automated Decision Making Technology. The DPIA will assess any data risks associated with the processing.

As Automated Decision Making Technology is generally considered to be 'high risk', the Data Protection Officer must sign and authorise the DPIA prior to the commencement of the processing.

Data Processors Using Automated Decision Making Technology

Where the council employs a Data Processor to utilise Automated Decision Making Technology it must ensure it has completed and had approved a Data Protection Impact Assessment, agreed to Data Processing clauses, and agreed a process of appeals prior to the processing taking place.

The council will record all instances of Data Processors using Automated Decision Making Technology on its Information Asset Register and Register of Automated Decision Making Technology.

Appendix 1

Standard data processing clauses

The Council must ensure that all of its contracts, where a third party will be processing data on the Council's behalf, contain the following criteria:

Mandatory Details

- the subject matter and duration of the processing
- the nature and purpose of the processing
- the type of personal data and categories of data subject.

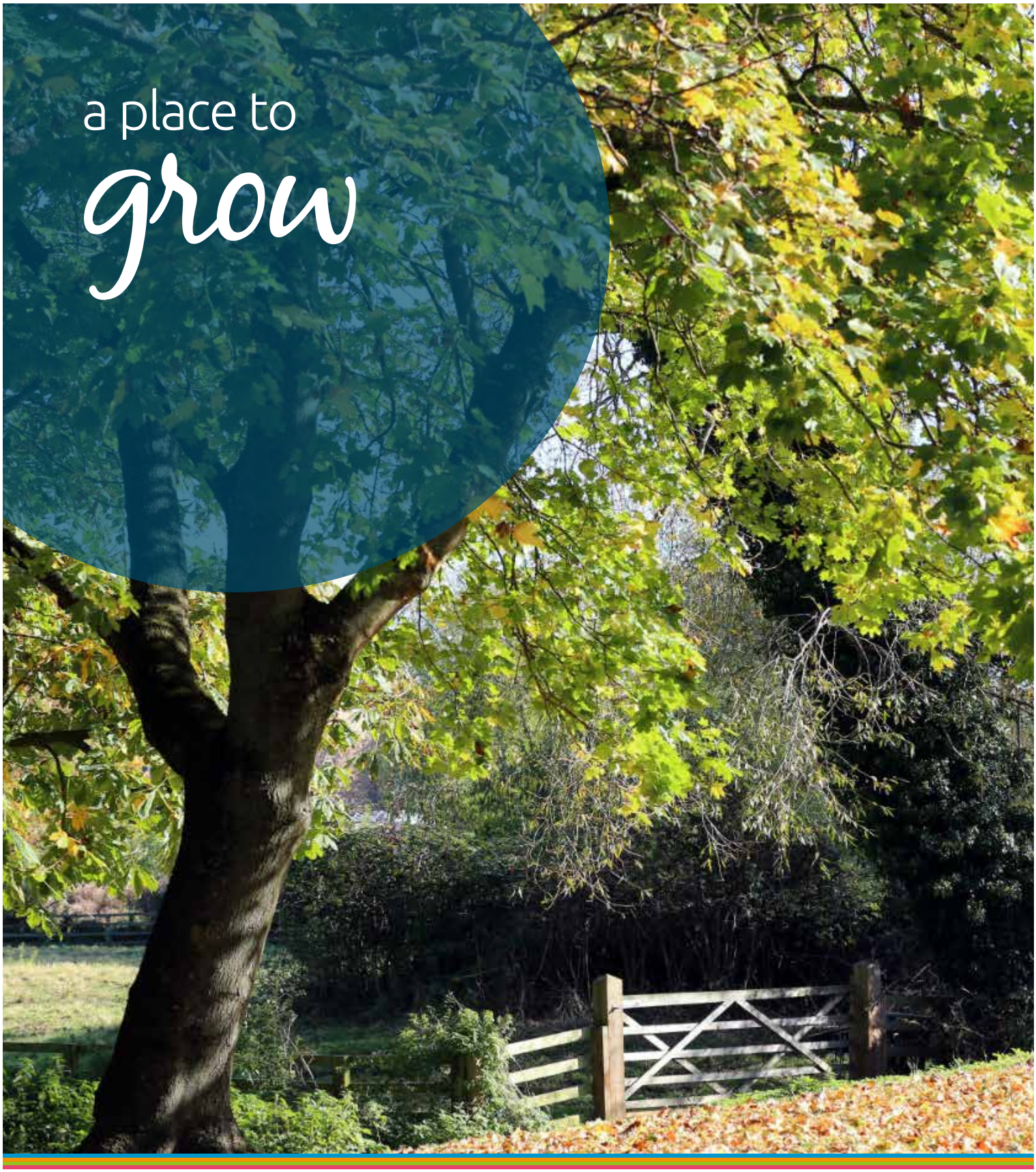
Mandatory Terms

- the processor must only act on the written instructions of the controller (unless required by law to act without such instructions)
- the processor must ensure that people processing the data (employees) are subject to a duty of confidence
- the processor must take appropriate measures to ensure the security of processing
- the processor must only engage a sub-processor (i.e a third party organisation) with the prior consent of the data controller and a written contract
- the processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the GDPR
- the processor must assist the data controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches, and data protection impact assessments
- the processor must delete or return all personal data to the controller as requested at the end of the contract (with an explanation as to method of destruction or return)
- the processor must submit to audits and inspections, provide the controller with whatever information it needs, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

Best Practice

- that nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR
- reference to any indemnity that has been agreed.

The Council's DPO will maintain template clauses as well as an assessment checklist for clauses that originate from the third party.



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