Alliance Data Protection Policy

1. Introduction

1.1 High Peak Borough Council and Staffordshire Moorlands District Council ("The Councils") collect and use information about people to efficiently and effectively provide quality services. The Councils may also be required by law to collect and use certain information.

1.2 This may be information about:

- members of the public;
- businesses;
- customers; and
- current, past and prospective employees and Councillors.

1.3 It is important that the collection and use of personal data is carried out lawfully, fairly and in a transparent manner. Failure to do so can lead to a range of problems including poor decision making, inefficient business processes, inconvenience or harm to residents and others, reputational damage to the authority, or enforcement action by the Information Commissioner's Office. Enforcement action can include fines of up to 10 million Euros[1] for serious breaches of data protection legislation and prosecution for deliberate breaches.

1.4 The key sources of data protection legislation are:

- The Data Protection Act 2018; and
- General Data Protection Regulation (GDPR) (EU 2016/679).

1.5 The Councils are fully committed to compliance with data protection requirements, which controls the way information is handled and gives legal rights to people who have information stored about them.

1.6 Explanations of key terms are provided at Appendix A.

[1] Approximately £8,800,000

2. General Principles

2.1 The GDPR specifies six key principles to be followed when processing personal data[2].

	Principles	Actions
a	*lawfulness, fairness and transparency* • processed lawfully, fairly and in a transparent manner in relation to the data subject	• Information should only be held where it is justified to do so and processing may be carried out where one of the following conditions has been met: a) Consent: The individual has given clear consent for you to process their personal data for a specific purpose. b) Contract: The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. c) Legal obligation: The processing is necessary for you to comply with the law (not including contractual obligations). d) Vital interests: The processing is necessary to protect someone's life. e) Public task: The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. f) Legitimate interests: The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. • The Councils will generally rely on 'legal obligation' (c) and 'public task' (e) when processing data. Councillors will normally rely on 'public task' when carrying out casework on behalf of their constituents. • Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data. • Handle people's personal data only in ways they would reasonably expect.
b	*purpose limitation* • collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	• Each Council is one data controller. As such, personal data held by the Council can be used within the Council, as set out in the Councils' Privacy Notice, to carry out the functions of the Council. • Access to personal data is restricted to those within the Council that need access to it for an

[2] Set out at Article 5.

		identified lawful purpose (a to f above). • If you wish to use or disclose personal data for any purpose that is additional to or different from the originally specified purpose, make sure that the new use or disclosure is fair. • When receiving requests for personal data, clarify the identity of the requesting party, the reason why the information is required and if there is authority to give the personal data (section 6). • Where consent is used as the legal basis for processing personal data, you must ensure that consent is unambiguous, freely given and an affirmative action. You must maintain an audit trail to demonstrate that consent was gained and have systems that allow consent to be revoked. Where special category data are processed, the consent gained will be explicit consent.
c	*data minimisation* • adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• Hold the minimum personal data required to perform the function that you need it for. • Do not hold more information than you need.
d	*accuracy* • accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay	• Take reasonable steps to ensure that information is accurate and up-to-date.
e	*storage limitation* • kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed	• Refer to the Councils' Document Retention Policy; • Securely delete information that is no longer required.
f	*integrity and confidentiality* • processed in a manner that ensures appropriate security of the personal data, including	• Follow the Councils' ICT Use and Information Security Policy • Identify potential risks and put appropriate measures in place.

	protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.	• Report breaches of security.

2.2 The Councils will ensure that data is processed in accordance with the rights of the data subject set out in the GDPR including the:

- Right of access.
- Right to rectification.
- Right to erasure.
- Right to restriction of processing.
- Right to data portability.
- Right to object.

3. Responsibilities for processing personal data

3.1 All staff members, Councillors and the Councils' contractors must take reasonable steps to make sure that personal data is processed in accordance with the data protection principles. To support this, the Councils will:

- Identify a member of the Senior Management Team to act as Senior Information Risk Officer (SIRO) with overall responsibility for overseeing the Councils' response to information risk;
- Identify a Data Protection Officer to develop the Councils' response to information risk and act as a source of expertise within the Council;
- Develop a Data Protection Policy, ensure awareness of the policy, and monitor its implementation;
- Hold quarterly Information Risk Group meetings, attended by the owners of the Councils' information assets (eg CCTV, Council Tax, Housing, Revenues and Benefits systems, etc) to identify possible risks and take steps to mitigate against such risks;
- Provide induction training and regular refresher training for all staff with more in-depth training for key owners of the Councils' information assets;
- Require Council officers to consider the data protection implications, and the potential need to complete a privacy impact assessment (see below), within each committee report;
- Ensure that appropriate physical and technological security measures are put in place;
- Establish a system for responding to Subject Access Requests (Section 8) and monitor compliance with the system;

- Register the way in which each Council processes personal information with the Information Commissioner[3]; and
- Carry out regular checks of services' compliance with this policy.

Staff Members

3.2 Individual officers will be expected to pay regard to the data protection principles and accompanying steps outlined in Section 2 and must follow the Councils' ICT Use and Information Security Policy. They must also take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data are collected for a legitimate purpose (or purposes) and are accurate, up to date and deleted in accordance with the Councils' data retention policy when no longer needed;
- A record is maintained of information held by each service to ensure fair and lawful processing;
- All names and addresses (postal or e-mail) are checked to make sure that they are correct and up to date before any personal information is sent to others;
- The secure (pin controlled) printing facility is used, where possible, and personal information is not allowed to sit uncollected on printers;
- The Councils' clean desk policy is complied with and personal information is not left unattended on desks;
- Personal information collected by the Councils is not transferred to, or stored upon, equipment owned by staff members (computers, laptops, tablets, smart phones, etc);
- Personal information is only transported between locations where absolutely necessary and that, when doing so, appropriate levels of security are applied (eg not leaving folders containing personal information unattended in cars or bags, ensuring that memory sticks are encrypted/password protected, etc);
- Any losses of data are reported promptly to the Data Protection Officer; and
- Requests for personal information are responded to in line with the process established in Section 4.

Service Managers

3.3 In addition, Service Managers must:

- Implement this policy within their Service area;
- Ensure compliance with it by staff members, including raising awareness of data protection responsibilities;

[3] In accordance with the Data Protection (Charges and Information) Regulations 2018

- Ensure that the Service's information asset register is accurate and up-to-date;
- Understand the information risks related to the Service's processing of data and take steps to manage any risks effectively;
- Ensure that all data breaches are reported to the Data Protection Officer without undue delay (Section 4);
- Ensure that appropriate privacy notices are provided to customers;
- Check the accuracy, completeness and appropriateness of any information to be provided by the Service in response to a request for information (Section 8) before it is sent to the Data Protection Officer; and
- Ensure all contractors use by the Service have suitable processes in place to comply with data protection legislation and that they know how and when to report any breaches.

Councillors

3.4 Councillors may perform three different roles:

• As a member of the council	eg when attending Council committees or performing an Executive role	This is covered by the Councils' ICO registrations and this policy
• Carrying out casework on behalf of their constituents	eg when recording and passing on complaints received from constituents	This is not covered by the Councils' ICO registrations. Councillors do not need pay a charge to register with the ICO for processing data[4].
• Representing a political party (particularly at election time).	eg campaigning during an election period	This is not covered by the Councils' ICO registrations or this policy. Any necessary registrations, etc are normally provided by individual political parties.

3.5 When Councillors consider using personal information then they should:

- decide whether their use of the information would be fair and lawful as required by the first data protection principle;

[4] From 1 April 2019, the Data Protection (Charges and Information) (Amendment) Regulations 2019 exempted the processing of personal data by elected representatives and prospective representatives from the requirement to notify the ICO and pay a charge.

- ensure that personal information held by the local authority is not used for political purposes unless both the local authority and individuals concerned agree; and
- when campaigning for election, candidates can normally use personal information (such as mailing lists) held by their parties but should not use information they hold in their role as local councillors without the consent of the individual.

3.6 If an individual resident requests a councillor to take action on their behalf then the councillor's actions will normally be lawful on the basis that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (public task). This includes activity that supports or promotes democratic engagement.[5] Councillors should, however, ensure that they are open and transparent about their use of data. This can be achieved by using an appropriate privacy notice.

3.7 Councillors are able to process special categories of personal data (eg to pass the details of a complaint to officers of the Council for them to investigate and respond appropriately) without explicit consent[6].

3.8 The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 provides a basis for:

- Processing of sensitive personal data by elected members in connection with their functions as an elected representative, including the disclosure of such information where necessary; and

- Disclosure of sensitive personal data by organisations responding to Members acting on behalf of individual constituents.

3.9 The Order does not place an obligation on organisations to disclose sensitive personal data to elected members who raise matters on behalf of constituents but provides a legal basis for doing so.

3.10 If there is any doubt about the resident's wishes then it would be appropriate to obtain explicit consent from the resident for sharing and disclosing the information.

3.11 Candidates for election should be aware that political campaigning falls within the definition of direct marketing.

3.12 Further guidance can be found on the Information Commissioner's website: https://ico.org.uk/media/for-organisations/documents/1432067/advice-for-elected-and-prospective-councillors.pdf

[5] Section 8 (e), Data Protection 2018

[6] Article 9(2) of the GDPR; Section 8, Data Protection Act 2018;

Contractors

3.13 Council contract managers should ensure that any contractors, consultants, partners or other servants or agents of the Council, together with their staff who have access to personal data held or processed for or on behalf of the Council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under data protection legislation. This also applies to the suppliers of ICT systems and services which are designed to store, or process, personal data collected by the local authority. Where necessary contracts should:

- Ensure that any breach of any provision of legislation and/or this policy will be deemed as being a breach of any contract between the Council and that individual, company, partner or firm;
- Require suppliers to demonstrate that they meet the technical requirements prescribed by the Government's Cyber Essentials Scheme. The requirements can be found at: https://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf
- Allow data protection audits by the Council of data held on its behalf (if requested);
- Report any breaches to the appropriate Council contract manager and Data Protection Officer without undue delay; and
- Indemnify as appropriate the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages.

3.14 All contractors who process personal information supplied by the Council will be required, where necessary to confirm prior to entering into a contract that they will abide by the requirements of data protection legislation and this policy.

4. Breaches

4.1 A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed [7].

4.2 All suspected breaches should be reported without undue delay to the Councils' Data Protection Officer using the Data Incident Reporting Form that can be accessed on the intranet at https://hpbc.alliance-online.org/assured.

4.3 The Council has 72 hours to report a breach to the Information Commissioner unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

[7] Defined by Article 4, General Data Protection Regulation 2016.

4.4 The Data Protection Officer will record the breach and make a decision as to whether the breach should be reported. Where required, the DPO will work with the service area to examine whether steps could be taken to prevent re-occurrence of the breach in the future. The referral should describe:

- incident details;
- date and time of incident;
- details of person affected;
- whether the data subjects are aware of the breach
- the likely consequence of the breach; and
- measures taken to address/mitigate the breach.

4.5 Details of the number and types of breaches will be shared with the Councils' Information Governance Group. This group will, amongst other things, look for any patterns or repeat occurrences and consider what could be done corporately to mitigate against any future personal data breaches.

4.6 If the data breach is likely to result in a risk to the rights and freedoms of the data subject, then the authority is required to report the breach to the Information Commissioner, where feasible, within 72 hours of becoming aware of it. The Data Protection Officer will be responsible for making such referrals in consultation with the SIRO (or, in his absence, another Executive Director).

5. Communicating Privacy Information to Individuals

5.1 The Councils (and Councillors when carrying out casework) must provide certain information when personal data are collected from the data subject [8]. This links to the requirement for transparency in the first data protection principle. The data subject should be provided with the following information at the time when the personal data are obtained:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) details of the legitimate interests pursued by the controller or by a third party where this is relied upon to lawfully process the data;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and related information.

5.2 A similar set of information must be provided to the data subject when the information has not been received from the data subject.

[8] Article 13, GDPR

5.3 The Council must actively communicate privacy information by taking positive action to provide such information. For example, by providing interactive information in an online form explaining why we need particular details. This could also be delivered via text-based notifications that appear briefly when an individual hovers over a particular field. This is different from having privacy information available for members of the public if they look for it themselves, for example by clicking on a web link or searching for more information on a website.

5.4 The need to actively communicate privacy information is strongest where:

- we are collecting sensitive information;
- the intended use of the information is likely to be unexpected or objectionable;
- providing personal information, or failing to do so, will have a significant effect on the individual; or
- the information will be shared with another organisation in a way that individuals would not expect.

5.5 The ICO suggests that rather than having a single, catch-all privacy notice, separate notices aimed at different groups are likely to make information clearer and easier to understand.

5.6 The Information Commissioner's Office has published guidance on privacy notices, transparency and control, which can be accessed at: https://ico.org.uk/about-the-ico/privacy-notices-transparency-and-control.

6. Data Sharing

6.1 Data sharing means the disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. It is recognised that data sharing across each Council and with other organisations can play a crucial role in providing better, more efficient services for our residents, businesses and others. However, it is important that we do this in the right way, and for the right reasons, and respect individual's rights under the Data Protection Act.

6.2 Two data sharing checklists, based upon those published by the ICO, are provided at Appendix B. One should be used for the 'systematic' sharing of data, which generally involves the routine sharing of data sets for an agreed purpose, and the other is for ad hoc (or one-off) data sharing. Anyone considering sharing of data with others should consider the relevant checklist before disclosing any personal data.

6.3 The Councils may have express obligations, or expressed or implied powers within legislation to share personal information. In other cases, data sharing may not involve personal data, for example where only statistics that cannot identify anyone are being shared. It is still important for the authority to seek to be transparent about the sharing of personal

information in such circumstances, wherever appropriate, as outlined in the previous section.

6.4 The general rule is that individuals should, at least, be aware that personal data about them has been, or is going to be shared. This applies even if the individual's consent is not needed. There are certain limited circumstances under which personal data, even sensitive data, can be shared without the individual knowing about it. This includes:

- the prevention or detection of crime
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty.

6.5 An organisation processing personal data for one of these purposes is exempt from the fairness requirements of the Data Protection Act, **but only to the extent that applying these provisions would be likely to prejudice the crime and taxation purposes.**

6.6 The authority needs to have an auditable record of any information that has been requested by or from others, the decisions whether or not to disclose the requested information and the reasons for that decision.

6.7 Appendix C provides a standard data request form. This should be used by external agencies or organisations when requesting third party information from the Council. It can also be used for requesting information from other organisations where they do not have their own specific form to complete.

6.8 Appendix D provides a template to be used to record decisions about whether to share information following a request from another organisation. It is important that you use this to keep a record of your decision-making process.

6.10 The Information Commissioner has produced a code of practice on data sharing, which can be accessed at: *https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/*

7. Privacy Impact Assessments

7.1 The Council will consider the potential impact of any project that involves the use of personal data, or any other activity that could have an impact on the privacy of individuals, within its decision making processes. The Council will carry out a written Privacy Impact Assessment (PIA) where the potential impact on privacy is high, such as where:

- A new IT system for storing and accessing personal data is being considered;
- A data sharing initiative is being developed where two or more organisations seek to pool or link sets of personal data;

- A project seeks to identify people in a particular group or demographic and initiate a course of action;
- Existing data may be used for a new and unexpected or more intrusive purpose;
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding automatic number plate recognition capabilities to existing CCTV) is being considered;
- A new database that consolidates information held by separate parts of an organisation is being developed;
- Legislation, policy or strategies is being introduced which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

7.2 The PIA will look at information flows, identify the privacy and related risks, and identify and evaluate the privacy solutions. The PIA should be signed-off by the Councils' Senior Information Risk Officer (SIRO) and any outcomes built into the project plan.

8 Dealing with access requests

8.1 A data subject has the right to obtain confirmation from the Councils whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source; and

(h) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

8.2 The Councils have created a webform for use by people wishing to submit a data access request https://sar.infreemation.co.uk/highpeak/. Any requests that are received in writing should be sent to dpo@highpeak.gov.uk.

8.3 The Councils will require any individual who is making a request for information, other than those already known to the Councils, to provide proof of identity. This will normally involve providing:

- a government document which verifies the client's full name and a supporting document (eg a utility/Council Tax bill, bank statement, insurance certificate) which verifies their name and either their address or their date of birth.

8.4 The Councils must respond to a subject access request promptly and in any event within **one calendar month** of receiving it[9]. We may need to ask for more information to help it find the data or identify the person main the request. In such cases, the response period begins once we have all the necessary information to dealing with the request.

8.5 We can restrict access to someone's personal data, where it is a necessary and proportionate measure to:

(a) avoid obstructing an official or legal inquiry, investigation or procedure;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

Third Party Requests

8.6 In addition to subject access requests, the Councils also receive requests for data relating to individuals from third parties. The Councils can only share such information if there is a lawful reason for doing so. Such requests can be broadly grouped into two different types:

a) Subject Access Requests submitted on behalf of somebody else.

8.7 Information can only be released if the person requesting the information can provide proof that they are legally authorised to act on the data subject's behalf. This could be in the form of a letter of authority, lasting power of attorney, evidence of parental responsibility, etc. The Councils will not release information in such circumstances if it is not satisfied that the person requesting the information has provided sufficient proof of authorisation. The Councils may contact the data subject to verify that they are happy for the requested data to be released.

[9] S54 Data Protection Act 2018

b) Requests for personal data relating to another individual.

8.8 The Council can only release personal data relating to another individual if there is a lawful justification for doing so. Part 4 and Schedule 7 of the Act contain several specific exemptions to the disclosure/non-disclosure rules. As noted above, this includes information relating to crime and taxation, some regulatory activity and that linked to legal proceedings.

8.9 The Council will only release personal information relating to a third party if it receives a request in writing that clearly outlines why the person requesting the information believes that the data is exempt from the non-disclosure provisions. The Council needs to satisfy itself that such requests are legitimate and that the stated non-disclosure exemptions apply in that specific instance.

8.10 A clear record of the nature of the request and reasons for decision about release of information relating to their service need to be maintained by the relevant Service Manager. Information should only be released with the agreement of the Service Manager and the Data Protection Officer should be consulted if there is any uncertainty as to whether information should or should not be released.

9. Information security procedures

9.1 Data Protection Principle 7 requires the Councils to have appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

9.2 All staff members and Councillors are expected to follow the ICT Use and Security Policy. Key actions include:

- Choosing a password of suitable complexity that cannot easily be guessed;
- Not disclosing passwords to any other person;
- Not leaving desktop PC/terminal equipment unattended whilst still logged onto the system;
- Only running software that you are authorised to use and not installing any software onto a PC;
- Following the Internet and E-mail Usage policy;
- Suitably marking e-mails containing Protected or Restricted data in the subject line;
- Reporting information security incidents and/or security breaches immediately to the Information Security Officer and/or IT Service. This includes theft or loss of equipment and/or data;
- Not allowing individuals that you don’t know to pass unchallenged through a secure door;
- Supervising visitors; and

- Challenging people who are not wearing their identification or a visitor's badge.

10. Contact details

Data Protection Officer High Peak Borough Council Buxton Town Hall Market Place Buxton Derbyshire SK17 6EL dpo@highpeak.gov.uk	Data Protection Officer Staffordshire Moorlands District Council Moorlands House Leek Staffordshire ST13 6HQ dpo@staffsmoorlands.gov.uk

Appendix A Definitions

‘**Personal data**’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

‘**Special categories of personal data**’ means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data; biometric data; health data; or data concerning a natural person's sex life or sexual orientation.

‘**Processing**’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

‘**Restriction of processing**’ means the marking of stored personal data with the aim of limiting their processing in the future.

‘**Profiling**’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

‘**Pseudonymisation**’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

‘**Filing system**’ means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

‘**Controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

‘**Processor**’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘**Recipient**’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

‘**Third party**’ means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

‘**Consent**’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

‘**Personal data breach**’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Appendix B Data sharing checklist

Systematic Data Sharing

You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- Any relevant functions or powers of the organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

It is good practice to have a data sharing agreement in place.

As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Data Sharing Checklist – One-off Requests

You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?

Key points to consider:

- Any relevant functions or powers of the organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

Appendix C Data Sharing Forms

Request for disclosure of personal information

(1) Give the name of the organisation from which you are requesting information.

Organisation requiring information	

WHOSE INFORMATION ARE YOU REQUESTING?

(2) Give details of the person whose information you are requesting

Use the box below to give sufficient information for the Data Controller to identify an individual from their records. You should include the name and address of the individual and any other information you feel is relevant.

This must not be used for 'trawling' information and such requests will be refused

Name	
Address	
Other relevant information	

WHAT INFORMATION ARE YOU REQUESTING?

(3) Provide details of the information that you would like to receive

Use the box below to state what information you require to support your enquiry. You should not ask for 'all information known about individual' or similar. You must ask for specific information. Give enough information so the Data Controller can make a decision whether to disclose in accordance with your declaration at Para 4.

WHY DO YOU NEED THE INFORMATION?

(4) Tick on or more boxes below to confirm the purpose of requesting the information:

☐ the prevention or detection of crime

☐ the apprehension or prosecution of offenders

☐ the assessment or collection of a tax or duty or an imposition of a similar nature

☐ the maintenance of effective immigration control

☐ the investigation or detection of activities that would undermine the maintenance of effective immigration control; or

☐ the information is required to be disclosed by law etc or in connection with legal proceedings

Use the box below to provide details of the investigation/prosecution or assessment or collection, etc. explanation as to why the information is required for the purpose identified at (4) above.

Please provide the case number, file number, case name or other reference that identifies the investigation	

(5) How will failure to disclose the information prejudice the purpose identified at (4) above?

(6) Detail all other means of obtaining the information which you have used and are now exhausted and proved unsuccessful:

Declaration:
I certify that:

- Information is needed for the purpose(s) indicated in section 4.
- Information requested will only be used for the stated purpose(s).
- I am authorised to request this information on behalf of my agency or organisation.
- I will ensure that any data provided is processed according to data protection legislation. This includes but is not limited to ensuring that the information is securely stored and deleted when no longer required.
- Non-disclosure would prejudice the case.
- The information given on this form is correct to the best of my knowledge and belief
- I am aware of the provisions of Section 170 of the Data Protection Act 2018 regarding the unlawful obtaining of personal data, and that it is a criminal offence to obtain data without express legal gateway or permission of the data subject.

Name of Requestor	
Position/Job Title	
Address	
Contact Number:	
E-mail	
Signed	
Date	

This application must be authorised by an officer senior to the requesting officer. THIS REQUEST SHALL BE TREATED IN CONFIDENCE. Verification of the Requestor may be required upon request.

Please send the completed form to dpo@highpeak.gov.uk.

Please note: There is no statutory time limit within which local authorities are obliged to respond to requests made.

ELECTRONIC INPUT AND SUBMISSION
The email history will constitute an audit trail of confirmation and authorisation in the same way as wet signatures.

Appendix D Data Sharing Decision Form

Record of Decision to Share/Not Share Information

Who requested the information? (Name of individual and organisation)	
What information was requested	
What was the information needed for	
What information was shared?	
What was your justification for sharing/not sharing?	
Was the information shared with or without consent?	

Name: _____

Job title: _____

Service: _____