Data Protection Policy

1. Introduction

1.1 High Peak Borough Council has to collect and use information about people to efficiently and effectively provide quality services for the local area. The Council may also be required by law to collect and use information to comply with the requirements of central government. This information collected by the authority may include information about members of the public and businesses; customers and suppliers; and current, past and prospective employees and Councillors.

1.2 It is important that this collection and use of personal data is carried out lawfully, accurately and fairly. 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 £500,000 for serious breaches of the Data Protection Act 1998 ("the Act") and possible prison sentences for deliberate breaches.

1.3 High Peak Borough Council is fully committed to compliance with the requirements of the Data Protection Act, which controls the way information is handled and gives legal rights to people who have information stored about them.

2. General Principles

2.1 The Act stipulates that anyone processing personal data must comply with eight data protection principles. These principles are legally enforceable and require that:

	Data Protection Principle	In practice, you/the Council must:
1	Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met	• have legitimate grounds for collecting and using the personal data; • make sure that the individual whom the personal data is about has explicitly consented to the processing unless a relevant exemption applies; • not use the data in ways that have unjustified adverse effects on the individuals concerned; • 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; and • make sure you do not do anything unlawful

		with the data.
2	Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	• be clear from the outset about why you are collecting personal data and what you intend to do with it; • comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data; • comply with what the Act says about notifying the Information Commissioner; and • ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.
3	Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	• only hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and • ensure that you do not hold more information than you need for that purpose.
4	Personal data shall be accurate and, where necessary, kept up to date.	• take reasonable steps to ensure the accuracy of any personal data you obtain; • ensure that the source of any personal data is clear; • carefully consider any challenges to the accuracy of information; and • consider whether it is necessary to update the information.
5	Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	• review the length of time you keep personal data; • consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it; • securely delete information that is no longer needed for this purpose or these purposes; and • update, archive or securely delete information if it goes out of date.
6	Personal data shall be processed in accordance with the rights of data subjects under this Act.	• allow individual's access to a copy of the information comprised in their personal data; • provide an opportunity to object to processing that is likely to cause or is causing damage or distress; • allow an individual to prevent processing for direct marketing;

		• allow individuals to object to decisions being taken by automated means; and • allow people to have inaccurate personal data rectified, blocked, erased or destroyed. • (an individual also has a right to claim compensation for damages caused by a breach of the Act).
7	Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	• design and organise security to fit the nature of the personal data you hold and the harm that may result from a security breach; • be clear about who in the organisation is responsible for ensuring information security; • make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and • be ready to respond to any breach of security swiftly and effectively.
8	Personal data shall not be transferred to a country or territory outside the European Economic Area[1] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	• contact the Data Protection Officer before sending any personal data outside the EEA

2.2 Explanations of various key terms within the Act are provided at Appendix A.

3. Staff and Councillor responsibility for personal data

Staff Members

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

- Identify a member of the Senior Management Team to act as Senior Information Risk Officer (SIRO) with overall responsibility for overseeing the Council's response to information risk;
- Identify a Data Protection Officer to develop the Council's 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;

[1] The European Economic Area[1] includes the EU member states plus Iceland, Liechtenstein and Norway.

- Hold quarterly Information Risk Group meetings, attended by the owners of the Council's 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 on the requirements of the Data Protection Act, with more frequent training for key owners of the Council's 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 the Council processes personal information with the Information Commissioner; and
- Carry out regular checks of services' compliance with this policy.

3.2 Individual officers will be expected to pay regard to the data protection principles, and accompanying steps, outlined in Section 2. All managers and staff members must follow the Council's 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 Council's 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 Council's clean desk policy is complied with and personal information is not left unattended on desks;
- Personal information collected by the Council 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.

3.3 Where appropriate, Council contracts 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 the Act. 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 the Act 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);
- Indemnify as appropriate the Council against any prosecutions, claims, proceedings, actions or payments of compensation or damages.

3.4 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 the Act and this policy.

Councillors

3.5 Councillors may perform three different roles:

- As a member of the council
- As representative of residents of their ward
- Representing a political party (particularly at election time).

3.6 When operating as a member of the council, such as acting as a member of a committee, then the Councillor is carrying out the local authority's functions and so does not need to register with the Information Commissioner in their own right. Councillors should follow the guidance set out in this policy when performing this role.

3.7 When acting on behalf of a political party then a Councillor will normally be able to rely on their party's registration (but independents will need to have their own registration). When councillors represent residents of their ward, they are likely to have to register in their own right. For example, if they use personal information to timetable surgery appointments or take forward complaints made by local residents.

3.8 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;
- make sure that they have the consent of a resident to share information if raising a complaint on their behalf;
- 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 residents without the consent of the individual.

3.9 If an individual resident requests a councillor to take action on their behalf then the councillor will usually have the implied consent to retain any relevant personal data provided by the individual, to disclose it appropriately, and to receive information relating to the individual from organisations (including the local authority) who are being complained about provided this is reasonably necessary to fulfil the requested action.

3.10 If there is any doubt about the residents' wishes, or the information is of a sensitive nature, 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/1432067/advice-for-elected-and-prospective-councillors.pdf

4. Breaches

4.1 A personal data breach is 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 (General Data Protection Regulation 2016).

4.2 All suspected breaches should be reported without undue delay to the Council's Data Protection Officer using the Data Incident Reporting Form that can be accessed on the intranet at http://hpbcnet/Organisational%20Development/newforms/form.asp. The Data Protection Officer will record the breach and, where required, 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.

4.3 Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the Council will communicate the breach to the individual(s) concerned without undue delay. The communication to the data subject will not occur where:

- The Council has implemented technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; or
- The Council has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subjects is no longer likely to materialise; or
- It would involve disproportionate effort. In such a case, there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.4 Details of the number and types of breaches will be shared with the Council's 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.

4.5 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 first data protection principle states that personal data should be processed fairly and lawfully. The Information Commissioner's Office (ICO) notes that fairness has two main elements:

- using information in a way that people would reasonably expect and thinking about the impact on them; and
- ensuring people know how their information will be used, for example by providing or making available privacy notices using the most appropriate mechanism and, in a digital context, on all the online platforms used to deliver services.

5.2 The basic legal requirement is to make sure people know who we are, what we intend to do with their information and who it will be shared with or disclosed to. When we collect data, we need to be clear why we need it and also to predict whether we are likely to do other things with it in the future. This requirement will generally be met by the authority through the use of

clear and effective privacy notices to inform individuals about what we do with personal data. The authority will also consider whether it is appropriate to use other techniques to supplement privacy notices, such as just-in-time notices[2], on a case-by-case basis.

5.3 The local authority cannot give an individual a choice about the processing of personal data if the collection and use of personal information is necessary to provide a service or carry out the transaction that the individual has requested. This includes where the individual cannot expect to receive what he or she has asked for unless any necessary processing of their personal information takes place; or because individuals are required by law to provide their personal details. In these cases, it is still important to be fair and transparent about the collection and use of the personal details.

5.4 In other cases, the Council must ensure that they unambiguously obtain consent for the collection of personal data. Consent must be freely given, specific and fully informed. Consent must also be revocable and we should have procedures in place to action and record it when this happens.

5.5 The authority 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.

5.6 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.

5.7 The ICO suggest 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.

5.8 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.

[2] Just-in-time notices work by appearing on the individual's screen at the point where they input personal data, providing a brief message explaining how the information they are about to provide will be used.

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 the authority 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 local authority 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. Many organisations will request information using their own data request templates. Similarly, some organisations will require the authority to use a specific template when requesting information from them. This is permissible as long as those requesting information from the Council provide the basic information contained in the form provided at Appendix C.

6.7 Appendix C provides a standard data request form. This should be used when requesting information from other organisations that do not provide or require

the Council to use a specific form. Appendix C also provides a template to be used to record decisions about whether to share information following a request from another organisation.

6.8 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 Council's Senior Information Risk Officer (SIRO) and any outcomes built into the project plan.

8 Dealing with access requests

8.1 Section 7 of the Data Protection Act creates a right of access to personal data ('the right of subject access') and the Act's sixth data protection principle requires the authority to process personal data in accordance with the rights the Act gives to individuals. Requests made under Section 7 of the DPA are commonly referred to as Subject Access Requests (SAR). It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee of £10 is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

8.2 An individual can also request information about the reasoning behind any automated decisions, such as a computer-generated decision or an assessment of performance at work.

8.3 A SAR must be made in writing. The Council has provided a standard form for people wishing to submit a request but the Council cannot insist that people use it (Appendix D). A separate form has been created for people who only wish to request access to CCTV footage (Appendix E).

8.4 The Council must respond to a subject access request promptly and in any event within 40 calendar days of receiving it or (if later) the date on which we receive:

- The fee;
- Any information that we reasonably need to find the personal data covered by the request; and
- Any information requested to confirm the requester's identity.

8.5 Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a subject access request. This may include personal data that are being processed for:

- the prevention or detection of crime,
- the capture or prosecution of offenders,
- the assessment or collection of tax or duty,
- protecting members of the public from dishonesty, malpractice, incompetence or seriously improper conduct, or in connection with health and safety; or
- use in legal proceedings (including prospective legal proceedings).

8.6 All Subject Access Requests should be sent to dpo@staffsmoorlands.gov.uk in the first instance. A flowchart showing the process that should be followed is provided at Appendix F.

Third Party Requests

8.7 In addition to subject access requests, the Council also receives requests for data relating to individuals from third parties. The Council 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.

8.8 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 Council 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 Council may contact the data subject to verify that they are happy for the requested data to be released.

b) Requests for personal data relating to another individual.

8.9 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.

8.10 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.

8.11 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 authority 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

Appendix A Definitions

Data means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record. For the local authority, this means information held for housing or social services purposes
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Personal data means data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that, where the ability to identify an individual depends partly on the data held and partly on other information (not necessarily data), the data held will still be “personal data”.

The definition of personal data also specifically includes opinions about the individual, or what is intended for them.

Sensitive personal data means personal data consisting of information as to –
a) the racial or ethnic origin of the data subject,

b) his political opinions,

c) his religious beliefs or other beliefs of a similar nature,

d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

e) his physical or mental health or condition,

f) his sexual life,

g) the commission or alleged commission by him of any offence, or

h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with even greater care than other personal data. In particular, if you are processing

sensitive personal data you must satisfy one or more of the conditions for processing which apply specifically to such data (Schedules 2 and 3 of the Act), as well as one of the general conditions which apply in every case. The nature of the data is also a factor in deciding what security is appropriate.

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including –
a) organisation, adaptation or alteration of the information or data,

b) retrieval, consultation or use of the information or data,

c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data.

The definition of processing is very wide and it is difficult to think of anything that the local authority might do with data that will not be processing.

Data subject means an individual who is the subject of personal data. In other words, the data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Act. Failure to do so risks enforcement action, even prosecution, and compensation claims from individuals.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Appendix B Data sharing checklist

Systematic data sharing

Scenario: 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

Scenario: 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

Data Sharing Request Form

High Peak Borough Council
working for our community

Request for Disclosure of Personal Information
Under Section 29 of the Data Protection Act 1998

I am an officer of High Peak Borough Council making enquiries for the purpose(s) of:

{amend has applicable}

- ***the prevention or detection of crime, .***
- ***the apprehension or prosecution of offenders,***
- ***the assessment or collection of any tax or duty or of any imposition of a similar nature.***

Nature of enquiry:

{Tell them why you need the information}

Name and position of person requesting data	
Date of request	
Data requested	
Date required by	
Any specific arrangements re: retention/deletion of data:	

I confirm that the information requested is required for the prevention or detection of crime, or for the apprehension or prosecution of offenders, and that failure to provide the information will, in my view, be likely to prejudice these matters

Signed:	
Dated:	

Name of organisation	
Name and position of person requesting data	
Date of request	
Reference to data sharing agreement	

Data requested	
Purpose	
Date required by	
Any specific arrangements re: retention/deletion of data:	
Signed:	
Dated:	

Data Sharing Decision Form

To be used by other organisations when requesting information from the authority.

The authority will accept requests submitted on organisations' own forms provided that any such requests include full details of who is making the request, the reason(s) why the information has been requested, and reference to any specific exemptions within the Data Protection Act 1998.

High Peak Borough Council
working for our community

Request for Disclosure of Personal Information

I am an officer of {*INSERT ORGANISATION*} making enquiries for the purpose(s) of:

- **{specify purposes}**

Nature of enquiry:

{Tell us why you need the information}

Name and position of person requesting data	
Date of request	
Data requested	
Date required by	
Any specific arrangements re: retention/deletion of data:	

I confirm that the information requested is required for the purposes outlined above.

Signed:	
Dated:	

Name of organisation	
Name and position of person requesting data	
Date of request	
Reference to data sharing agreement	
Data requested	
Purpose	

Date required by	
Any specific arrangements re: retention/deletion of data:	
Signed:	
Dated:	

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: _____

Appendix D Subject Access Request Form

Subject Access Request Form

Data Protection Act 1998

Under the Data Protection Act 1998, you (the "Data Subject") are entitled to request access to personal information held about you by High Peak Borough Council. Completing this form will assist us in locating your information quickly and efficiently.

Please note that you will be required to provide proof of your identity (see section 5) and pay a fee of £10 before your request is processed.

If you are **only** requesting CCTV images please use the separate CCTV subject access request form.

Section 1 Your Details

Surname/Family Name	
First Name(s)	
Title	
Previously known as (if applicable)	
Current Address	
Postcode	
Date of Birth	
Telephone Number	
E-Mail	

If you are requesting historical data, please provide details of any previous addresses to assist us to find the information that you are requesting.

Previous Address(es)	**Date of Occupancy**	
	From	**To**

Section 2 Whose information are you requesting?

My own (go to section 4)
Someone else's
Both my own and someone else's

Section 3 If you are requesting someone else's information, whose is it?
Please provide their details:

Surname/Family Name	
First Name(s)	
Title	
Previously known as (if applicable)	
Current Address	
Postcode	
Date of Birth	
Telephone Number	
E-Mail	

If you are requesting historical data, please provide details of any previous addresses to assist us to find the information that you are requesting.

Previous Address(es)	**Date of Occupancy**	
	From	**To**

What is your relationship to the data subject *(e.g. parent, carer, legal representative)*	
Do you have legal authority to request the data subject's information?	
If the data subject is under 16, do you have parental responsibility for them?	

You must provide proof that you are legally authorised to act on the data subject's behalf. This may be in the form of a letter of authority, lasting power of attorney, evidence of parental responsibility, etc.

You must also provide proof that you are the person authorised to act on behalf of the data subject by providing a copy of your birth certificate, Driving Licence or two utility bills.

Section 4 What information are you requesting?

Please help us deal with your request quickly and efficiently by giving as much detail as possible about the information you want. If possible, please restrict your request to a particular service, period of time or incident to enable us to respond to your request quickly and efficiently. If necessary continue this section on a separate page.

Department(s)/service(s) that you think hold the information that you are requesting (if known)	
Time periods that you are interested in	
Description of information that you want to see. Please include any known reference numbers	

Section 5 Proof of Identification and Entitlement

You must provide proof of your name and address so that we only give information to the correct person. We require two pieces of information showing your name and address. In some cases, such as if you are asking us to release information of a sensitive nature, further information may be required.

Recent (less than 3 months old) utility bill
Bank statement
Passport or Photo ID driving licence
Change of name document(s) if relevant

Under the Data Protection Act, only the data subject has the right to ask to see their own records. We normally expect the data access request to be made by the data subject. In some circumstances, the data subject may wish to appoint someone else to make the subject request on their behalf. In such cases, we will only release the data on receipt of proof of entitlement to request data on the data subject's behalf. This should include a letter of authority from the data subject.

Document(s) supplied as proof of entitlement. Please describe what document(s) you are providing.

Section 6 Payment

A fee of £10 must be paid before the Council will process your request for information.

Payment may be made by:

- Posting a personal cheque or postal order (made payable to **High Peak Borough Council)**, together with a copy of this form or a written request for information, to High Peak Borough Council, Buxton Town Hall, Market Place, Buxton, Derbyshire SK17 6EL or
- Visiting in person, bringing a copy of this form or a written request for information, and paying by credit/debit card personal cheque or postal order at the Council Offices in Glossop or Buxton.

Appendix E Subject Access Request Form (CCTV)

How to Apply For Access To Information Held On the CCTV System

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of the information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or data does not fall within the Data Protection Act 1998 or if you agree otherwise. High Peak Borough Council will only give that information if it is satisfied as to your identity.

If release of the information will disclose information relating to another individual(s), who can be identified from that information, the High Peak Borough Council is not obliged to comply with an access request unless –

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

High Peak Borough Council CCTV System Rights

High Peak Borough Council may deny access to information where the Act allows or does not apply. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders
- Where the Data protection Act 1998 does not apply (Where not used to capture identifiable individuals or information relating to individuals)

and giving you the information may be likely to prejudice any of these purposes.

Fee

A fee of £10 is payable for each access request, which must be in pounds sterling. Cheques, Postal Orders, etc. should be made payable to High Peak Borough Council

THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)

Section 1 Asks you to give information about yourself that will help us confirm your identity . We have a duty to ensure that information it holds is ensure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full photograph of you.

Section 3 The declaration must be signed by you.

When you have completed and checked this form, take or send it together with the required TWO identification documents, photograph and fee to: The CCTV Manager, High Peak Borough Council, Buxton Town Hall, Market Place, Buxton, Derbyshire SK17 6EL.

SECTION 1 About Yourself

The information requested below is to help us (a) satisfy itself as to your identity and (b) find any data held about you.

PLEASE USE BLOCK CAPITAL LETTERS

Title *(tick box as appropriate)*	Mr		Mrs		Miss		Ms	
Other title *(e.g. Dr., Rev., etc.)*								
Surname/family name								
First names								
Maiden name/former names								
Sex *(tick box)*	Female				Male			
Height								
Date of Birth								
Ethnicity								

Current address:	Post code:
Telephone number (in case we need to contact you)	

Previous address		
Date of occupancy	**From:**	**To:**
Previous address		
Date of occupancy	**From:**	**To:**
Previous address		
Date of occupancy	**From:**	**To:**

SECTION 2 PROOF OF IDENTITY

To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving license, medical card, passport or other official document that shows your name and address.

Also a recent, full face photograph of yourself .

Failure to provide this proof of identity may delay your application.

SECTION 3 SUPPLY OF INFORMATION

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

TICK ONE

(a) View the information and receive a permanent copy Yes ❐ No ❐

(b) Only view the information Yes ❐ No ❐

SECTION 4 DECLARATION

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signed by: _____ *Date:* _____

Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence

SECTION 5 TO HELP US FIND THE INFORMATION

If the information you have requested refers to a specific offence or incident, please complete this Section.

Were you: (tick box below as applicable)

A person reporting an offence or incident ❒

A witness to an offence or incident ❒

A victim of an offence ❒

A person accused or convicted of an offence ❒

Other – please explain

Dates(s) and time(s) of incidents	
Place incident happened	
Brief details	

If the information involves a vehicle then please complete the following:

Make	
Model	
Colour	
Registration number	
Other distinguishing features	

Please note: We will require proof that you own the vehicle or were in the vehicle at the time.

These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable from The Stationery Office. Further information and advice may be obtained from: The Office of the Information Commissioner, Wycliffe House, **Water Lane, Wilmslow, Cheshire, SK9 5AF.**

Please note that this application for access to information must be made direct to **High Peak Borough Council** and **NOT** to the Information Commissioner

OFFICIAL USE ONLY

Please complete ALL of this Section (refer to 'CHECK' box above).

Application checked and legible? ❒	Date Application Received
Identification documents checked? ❒	Fee Paid
Details of two documents	
Documents returned	❒
Officer name	
Date	

.

Appendix F Subject Access Request Flowchart