

Stocksfield Parish Council

Data Protection Policy

1. Introduction

Stocksfield Parish Council (the Council) collects and uses (collectively known as processing) a variety of information, including personal data, in order to perform its statutory functions. In the vast majority of cases, the personal data processed is limited to the name and contact details of the data subject although it can relate to any data that identifies a living individual. The Council recognises that the way it collects and handles data is critical to maintaining the confidence and trust of the community within Stocksfield. The Council, as data controller, will comply with the six principles in Article 5 of the General Data Protection Regulations (GDPR) (listed in Appendix A) and will process personal data in a fair and transparent manner which complies with the Data Protection Act 2018 (DPA) and the GDPR.

2. Processing of Personal Data

2.1 Purpose and manner

The Council will process personal data for the following purposes:

- Performance of its statutory duties and powers, including
 - the management of the Council's facilities and existing contracts,
 - the processing of relevant financial transactions including grant applications and payments for goods and services supplied to the Council,
 - the employment of staff,
 - the administration of members,
 - working in partnership with other public agencies, local and regional groups,
 - the conduct of appropriate safeguarding procedures,
 - the promotion of the interest of the Council,
 - the maintenance of the Council's records and accounts
 - sending data subjects information they have requested.
- Assessment of and response to the concerns of residents (whether or not in connection with a statutory duty or power) and, where the concern relates to a matter relevant to the Council, the concerns of non-residents
- Implementation of the aims and objectives detailed within the Council's Plan, as amended from time to time.

The processing of personal data for the purposes outlined allows the Council to provide an enhanced and effective service to its community and partners, and to respond appropriately to data subjects about matters of concern to them.

The Council processes personal data by collecting, recording, organising, structuring, adapting, retrieving, using, disclosing, disseminating, restricting, erasing or destroying data. The personal data which is or may be processed is listed below:

- Names, titles, contact details such as address, telephone number and email address
- Where they are relevant to the services provided by the Council, or where a person provides them, the Council may process information such as gender, age, marital status, nationality, education/work histories, family composition and dependants
- Where a person pays for activities or make application to the Council for funding, financial identifiers such as bank account numbers, payment transaction identifiers and claim numbers

- Where a person provides them to the Council and they are directly relevant to the purpose of the contact with that person, special category data (also known as sensitive information - see section 2.4)
- Where a person visits the Council's website, both 'persistent' and 'session' cookies are used to assist in the website's use, (eg by enhancing navigation or recording preferences about how a person previously viewed a webpage such as the size of text). Cookies cannot be used to identify an individual person.

In the majority of cases the personal data processed by the Council has been provided to the Council by the data subject. Electronic correspondence, together with any attachment, is filed by reference to email address, subject matter and date. All other electronic documents are filed by reference to the data subject's name. Paper records relating to personal data are digitised, unless impractical do to so. Electronic data, together with regular back up data is retained securely using suitable password protection. Back up data is protected against theft, fire and flood. Other 'relevant filing systems' are held securely in locked units. Data will be deleted in accordance with the Council's Guidelines for the Retention of Records.

2.2 Data processors

The Council will only use a data processor to process personal data on its behalf (ie a person or organisation other than an employee of the Council) where a written agreement exists which documents the relationship between the Council and data processor as required by GDPR.

2.3 Lawful basis

There are four bases upon which the Council relies for the lawful processing of personal data:

- *consent* – can be relied upon for any purpose but a controller must be able to demonstrate that consent was given.
- *contract* – necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of a data subject prior to entering into a contract,
- *legal obligation* - necessary for compliance with a legal obligation to which the controller is subject
- *public task* – necessary for the Council to perform a task in the public interest or for the Council's official functions, and the task or function has a clear basis in law

In general, where processing is in connection with a statutory duty or power, including activity under Section 137 Local Government Act 1972, '*legal obligation*' or '*public task*' are the lawful bases upon which the Council relies to process the data. However, where the processing also relates to the performance of a contract, the Council relies upon '*contract*' as the lawful basis. These three lawful bases are often overlapping. Where the Council processes personal data in order to keep data subjects informed of specified Council activities, '*consent*' will be the lawful basis upon which the Council relies to process that data.

A list of all available bases is shown at Appendix B. Charts showing the detail of the lawful bases relied upon by the Council to process personal data from differing categories of data subject are shown at Appendix C. The fact that particular categories of data subject and personal data are shown with a corresponding lawful basis for processing does not necessarily mean that the Council has processed or currently retains information in that category.

2.4 Special category data (or sensitive information)

The processing of special category data requires further consideration and must, in addition to the requirement in paragraph 2.3, comply with one of the conditions listed in Article 9(2) of GDPR. Appendix D lists the types of special category data and the additional conditions. The Council will not request special category data from data subjects unless there are exceptional circumstances. Special category data is generally processed only in the following two ways:

- i) Where a data subject contacts the Council to complain or raise any issue and, during that contact, reveals special category data about themselves which is specific and integral to the matter of concern raised, or
- ii) Where a data subject provides contact details including special category data about themselves to enable the Council to communicate with them about matters that relate to them as a consequence of the special category data revealed.

In respect of (i) above, the Council will regard the data subject as having consented explicitly to the Council processing that data for that specific purpose. Where the special category data is superfluous to the issue, it will be deleted. With regard to (ii) above, the Council will only process the special category data with the explicit consent of the data subject. Less commonly the Council may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect a person's interests and they are not capable of giving consent, or where they have already made the information public.

3. Rights of data subject

3.1 Access

A data subject has the right of access to the data held which means confirmation that data is held and access to it. Although there are exceptions, in general the data must be provided within one month of the request. Provision of the data is free although a reasonable fee may be charged where the request is manifestly unfounded, excessive or repetitive. In order to process any requests for access to personal data, the Council may need to verify a data subject's identity. Requests for such access can be made in writing or by email as listed below:

Stocksfield Parish Council,
(Subject Access),
Stocksfield Community Association
Mount View Terrace
Stocksfield
NE43 7HL

Email: subjectaccess@stocksfield-pc.gov.uk

The Council's Subject Access Request Procedure is an integral aspect of the Data Protection Policy and is shown at Appendix E.

3.2 Rectification

Data subjects have the right to rectification of inaccuracies which will be made within one month of the Council receiving a notice to rectify.

3.3 Erasure

Data subjects have the right to ask for erasure (or to be forgotten) and the Council will consider each request on its individual merits. Where a data subject demands erasure of personal data, including special category data, where it is held with the data subject's *consent*, the data will be erased immediately upon request and the data subject will be informed. In all other cases the

Council will consider the request and will confirm either that the data has been deleted or explain why it cannot be deleted (eg to comply with a *legal obligation*).

3.4 Portability

Data subjects have the right to request the transfer of some of their data to another controller where it is processed with *consent* or for the performance of a *contract*. Such a request will be complied with, where feasible, within one month.

3.5 Object

Data subjects have the right to object to processing where it occurs as a *public task* and the Council will consider such requests based on individual circumstances.

3.6 Privacy notice

The Council has adopted a privacy notice for members of the public (Appendix F) and an alternative privacy notice for staff, members and role holders, which includes volunteers and contractors (Appendix G). Both notices are displayed on the Council's website and relevant extracts have been incorporated into the standard signature on Council emails. The Council's consent form for processing of personal data is shown at Appendix H.

4. Disclosure

Where a person makes unsolicited contact with the Council in connection with the Council's statutory duties and powers or any other matter connected to the Council Plan, the Council may disclose personal data to its members (ie the elected councillors) only where that disclosure is necessary to enable the matter raised to be correctly addressed or the data subject has given their consent (including by email). The same principle applies where the unsolicited contact is direct to a member – the member must ensure that disclosure to the Council (including to other members) is necessary or the data subject has consented.

Where a person contacts the Council in response to a general consultation request from the Council, any views expressed will be presented in an anonymous format and no personal data will be disclosed.

No further disclosure of personal data will occur without the consent of the data subject unless such disclosure is required by law.

5. Data Security

It is the responsibility of all members and employees to ensure that their actions comply with the requirements imposed by GDPR and the DPA. In particular they must ensure that any personal data they hold, whether electronic or paper format, is kept secure and is not disclosed deliberately or accidentally to any unauthorised party, whether in writing or orally.

6. Retention of data

The Council has produced guidelines for the retention of records which are shown at Appendix I. They describe the timescales in which various categories of data are normally retained.

7. Personal data breaches

A 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. This includes breaches that are the result of both accidental and deliberate causes and extends breaches beyond simply losing data.

Where a member identifies a potential personal data breach they must inform the Clerk immediately. Certain data breaches (eg where there is a high risk to the individuals involved, for instance, through identity theft) must be notified to the ICO and the individual(s) concerned. It is the responsibility of the Clerk to assess the nature of the incident and where a breach has occurred, the Clerk is authorised to take whatever action is necessary to mitigate the breach. Where possible the Clerk will liaise with the Chair or the Vice Chair but their absence will not delay any necessary action by the Council. An assessment of the impact of the breach will be undertaken and will inform the necessary response.

Any data security breach is a serious matter and all breaches, no matter how minor, will be recorded by the Clerk and reported to the Council. The Clerk is responsible for reporting breaches when appropriate to the ICO after liaison with the Chair or Vice-Chair. The absence of either will not prevent notification within the required timescale.

In the absence of the Clerk, the Chair and Vice Chair have responsibility jointly for assessing any potential breach and jointly have delegated authority to take appropriate action.

8. Data Protection Officer

The Council has appointed a Data Protection Officer (DPO) whose role and responsibilities are described within GDPR and DPA. The data protection officer can be contacted by email: dpo@stocksfieldpc.org.uk.

Schedule of Appendices

- A** Principles of GDPR
- B** Lawful bases for processing personal data under GDPR
- C** Lawful bases relied upon by the Council
- D** Special category data
- E** Subject Access Request Procedure
- F** Privacy notice – members of the public
- G** Privacy notice – staff, members and role holders
- H** Consent form
- I** Guidelines for the retention of records

Related documents
Email and internet policy; Information Security Policy; Freedom of Information Publication Scheme

Adoption and Review History	
Adopted	14 May 2018
Reviewed	22 May 2024
Next review due	May 2029

Principles of the General Data Protection Regulations

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

Lawful bases for processing

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever personal data is processed:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **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.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life.
- **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.
- **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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Lawful bases relied upon by the data controller by data category and data subject

Processing in connection with a statutory power or duty of the data controller							
Type of personal data	Employees (current, past or prospective)	Members	Volunteers	Suppliers of goods and/or services	Recipients of services or facilities provided as part of a contract	Employees/ members of other partner/public agencies	Other persons, including residents and complainants, not otherwise listed
Name	Legal obligation	Legal	Legal/Public	Contract	Contract	Public task	Public task
Address	Legal	Legal	Legal/Public	Contract	Contract	Public task	Public task
Other contact details	Legal	Legal	Legal/Public	Contract	Contract	Public task	Public task
Age or date of birth	Legal	-	-	-	-	-	Public task
Financial	Legal	Legal	Legal/Public	Contract	Contract	Public task	Public task
Employment	Legal	Legal	-	Contract	-	Public task	Public task
Special category data	-	-	-	-	-	-	Public task

Other processing in connection with other defined purposes of the data controller							
Type of personal data	Employees (current, past or prospective)	Members	Volunteers	Prospective suppliers of goods and/or services	Employees/ members of other partner/public agencies	Other persons who decide to receive information from the Council	Other persons, including residents and complainants, not otherwise listed
Name	-	Public task	Public task	Public task	Public task	Consent	Public task
Address	-	Public task	Public task	Public task	Public task	Consent	Public task
Other contact details	-	-	Public task	Public task	Public task	Consent	Public task
Age or date of birth	-	-	-	-	-	Consent	Public task
Financial	-	-	Public task	-	Public task	-	-
Employment	-	-	Public task	-	Public task	-	-
Special category data	-	-	-	-	-	-	-

Special category data

Also referred to as sensitive personal data, special category data includes information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Additional conditions, one of which is required to process special category data in addition to a lawful basis referred to in Appendix B.

The conditions are listed in Article 9(2) of the GDPR:

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and

services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Stocksfield Parish Council

Subject Access Request Procedure

2. Introduction

Stocksfield Parish Council (the Council) is the data controller as defined by the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) and must comply with the requirements of both in respect of subject access requests (SAR). All individuals have the right to access their data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. This policy sets out the Council's role, its minimum standards and the roles of employees and members.

2. A subject access request

The Council provides a dedicated email address for the receipt of SARs (subjectaccess@stocksfield-pc.gov.uk) although data subjects may submit SARs in writing to the Council's office. Where an employee or member receives an email or written correspondence which appears to be a SAR, they must forward the request to the above email address or, if a written application, to the Clerk. The Clerk is responsible for maintaining a record of all SARs received, including requests that appear to be a SAR and which are later shown not to be. The Clerk will ensure that the request is made under data protection legislation, as opposed to other legislation such as freedom of information.

The Council will acknowledge receipt of the SAR. The Council must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by the council relating to the data subject. Where necessary the Clerk should clarify with the requestor what personal data they need. The requestor must supply their address and valid evidence to prove their identity. The Council will accept the following forms of identification (*indicates documents must be dated within the past 12 months, + indicates documents must be dated within the past 3 months):

- Current UK/EEA Passport
- UK Photocard Driving Licence (Full or Provisional)
- Firearms Licence / Shotgun Certificate
- EEA National Identity Card
- Full UK Paper Driving Licence
- State Benefits Entitlement Document*
- State Pension Entitlement Document*
- HMRC Tax Credit Document*
- Local Authority Benefit Document*
- State/Local Authority Educational Grant Document*
- HMRC Tax Notification Document
- Disabled Driver's Pass
- Financial Statement issued by bank, building society or credit card company+
- Judiciary Document such as a Notice of Hearing, Summons or Court Order
- Utility bill for supply of gas, electric, water or telephone landline+
- Most recent Mortgage Statement*
- Most recent council Tax Bill/Demand or Statement*

Tenancy Agreement

Building Society Passbook which shows a transaction in the last 3 months and your address

Depending on the degree to which personal data is organised and structured, the Clerk will search emails (including archived emails and those that have been deleted but are still recoverable), Word documents, spreadsheets, databases, systems, removable media (for example, memory sticks, floppy disks, CDs) and paper records in relevant filing systems. Where necessary the Clerk will request that members undertake individual searches of their records to identify relevant personal data relating to the data subject.

Where the Council does not process any data, the data subject will be informed accordingly.

Personal data will not be withheld data because it may be misunderstood but instead an explanation will be provided with the personal data. The Council will provide the personal data in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The personal data must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. Where necessary, the requester may agree that they will view the personal data on screen or inspect files on our premises. Any exempt personal data must be redacted from the released documents and explanation will be given as to why that personal data is being withheld.

All requests must be responded to within one calendar month of the SAR although where a response cannot be made within one month, an extension of another two months is permissible provided this is communicated to the data subject in a timely manner within the first month. Responses will be free of charge. Where a data subject makes unfounded, excessive or repetitive requests an administrative fee may be charged or the Council may refuse to act on the request. Where the Council cannot provide the information requested it will inform the data subject within the first month.

Where data on the data subject is processed, the following minimum information must be supplied:

- (i) the purposes of the processing;
- (ii) the categories of personal data concerned;
- (iii) the recipients or categories of recipients to whom personal data has been or will be disclosed;
- (iv) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
- (v) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (vi) the right to lodge a complaint with the Information Commissioners Office ("ICO");
- (vii) if the data has not been collected from the data subject: the source of such data;
- (viii) a copy of the personal data undergoing processing.

Where a requester is unhappy with a response, the Council will deal with the matter as a complaint. In responding to a complaint, the Council will advise the requestor that they may complain to the ICO if they remain unhappy with the outcome.

The Clerk will maintain the register of SARs which allows reporting on volume of SARs and compliance against the statutory timescale.

Stocksfield Parish Council

GENERAL PRIVACY NOTICE

Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (eg a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (eg a list of residents may contain their elector reference number rather than names but if a separate list of the elector reference numbers is used which gives the corresponding names to identify the resident in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Stocksfield Parish Council which is the data controller for your data.

Other data controllers the council works with:

- Local authorities including other parish and town councils
- Other public bodies such as the police
- Community groups
- Charities
- Other not for profit entities
- Contractors

We will only share your personal data with other bodies with your consent or where we are required to do so by law. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the Council and the other data controllers may be “joint data controllers” which means we are all collectively responsible to you for your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant data controller.

A description of what personal data the council processes and for what purposes is set out in this Privacy Notice.

The council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles and aliases;
- Contact details such as telephone numbers, addresses, and email addresses;
- Where they are relevant to the services provided by the Council, or where you provide them to us, we may process information such as gender, age, marital status, nationality, education/work history, academic/professional qualifications, hobbies, family composition, and dependants;

- Where you pay for activities such as use of Council facilities, make an application for funding to the Council or enter into any contract with the Council, we may process financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
- Where you provide us with personal data which includes sensitive or other special categories of personal data, such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medication/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation, we may process that information if it is directly relevant to the purpose of your contact with us.

How we use sensitive personal data?

- These types of data are described in the GDPR as “Special categories of data” and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data in very limited circumstances where you have voluntarily provided the data to us and the data is directly relevant to the purpose of your contact – in other words this is with your explicit written consent.
- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- In very rare circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do for you and inform you of other relevant services;
- To confirm your identity to provide some services;
- To contact you by post, email or telephone;
- To help us to build up a picture of how we are performing;

- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions;
- To enable us to meet all legal and statutory obligations and powers including any delegated functions;
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults-at-risk are provided with safe environments and generally as necessary to protect individuals from harm or injury;
- To promote the interests of the council;
- To maintain our own accounts and records;
- To seek your views, opinions or comments;
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders;
- To send you communications which you have requested and that may be of interest to you. These may include information about campaigns, appeals, other new projects or initiatives;
- To process relevant financial transactions including grants and payments for goods and services supplied to the council
- To allow the statistical analysis of data so we can plan the provision of services.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation or for the performance of tasks carried out by a public authority acting in the public interest which includes the discharge of the council's statutory functions, powers and duties. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the council's services. We will always take into account your interests and rights. This Privacy Notice sets out your rights and the council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you or an organisation that you represent, or to take steps to enter into such a contract. An example of this would be processing your data in connection with the use of sports facilities.

Sometimes the use of your personal data requires your consent (eg you may ask us to send you information about issues which interest you) and, when it does, we will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties with whom the council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is possible that we will need to share your data with some or all of the following but this will only be with your consent or where we are required to do so by law:

- The data controllers listed above under the heading "Other data controllers the council works with".
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community.

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. We will retain personal data provided to us unsolicited as part of normal correspondence for a period of 3 years plus the year the data was provided. It is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

- 1) *The right to access personal data we hold on you***
 - At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
 - There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.
- 2) *The right to correct and update the personal data we hold on you***
 - If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.
- 3) *The right to have your personal data erased***
 - If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
 - When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).
- 4) *The right to object to processing of your personal data or to restrict it to certain purposes only***
 - You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.
- 5) *The right to data portability***
 - You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.
- 6) *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained***
 - You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7) *The right to lodge a complaint with the Information Commissioner's Office.*

- You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

When exercising any of the rights listed above, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

Transfer of Data Abroad

Personal data will not be transferred to countries or territories outside the European Economic Area ("EEA") although our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page <https://stocksfield-pc.gov.uk/policies-and-procedures/>

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Broomley and Stocksfield Parish Council, Stocksfield Community Association, Mount View Terrace, Stocksfield, NE43 7HL

Email: For general enquiries – dpo@stocksfield-pc.gov.uk

For subject access requests – subjectaccess@stocksfield-pc.gov.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Stocksfield Parish Council

PRIVACY NOTICE

For staff*, councillors and role holders**

*“Staff” means employees, workers, agency staff and those retained on a temporary or permanent basis

**Includes, volunteers, contractors, agents, and other role holders within the council including former staff*and former councillors. This also includes applicants or candidates for any of these roles.

Your personal data – what is it?

“Personal data” is any information about a living individual which allows them to be identified from that data (for example a name, photograph, video, email address, or address). Identification can be directly using the data itself or by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify the staff in the first list then the first list will also be treated as personal data). The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA) and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This Privacy Notice is provided to you by Broomley and Stocksfield Parish Council which is the data controller for your data.

The council works together with:

- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC
- Staff pension providers
- Former and prospective employers
- Payroll services providers

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be “joint data controllers”. This means we are all responsible to you for how we process your data where for example two or more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

The council will comply with data protection law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.

- Kept only as long as necessary for the purposes we have told you about.
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

What data do we process?

- Names, titles, and aliases.
- Start date/leaving date
- Contact details such as telephone numbers, addresses, and email addresses.
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants.
- Non-financial identifiers such as passport numbers, taxpayer identification numbers, staff identification numbers, tax reference codes, and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers.
- Financial information such as National Insurance number, pay and pay records, tax code, tax and benefits contributions, expenses claimed.
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to, IP addresses and website visit histories, logs of visitors, and logs of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)
- Location of employment or workplace.
- Other staff data (not covered above) including; level, performance management information, languages and proficiency; licences/certificates, immigration status; employment status; information for disciplinary and grievance proceedings; and personal biographies.
- Information about your use of our information and communications systems.

We use your personal data for some or all of the following purposes: -

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.
- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any contractual benefits to you
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Conducting grievance or disciplinary proceedings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.

- Education, training and development requirements.
- Dealing with legal disputes involving you, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- Prevention of fraud.
- Monitoring your use of our information and communication systems to ensure compliance with our IT policies.
- Ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.
- Undertaking activity consistent with our statutory functions and powers including any delegated functions.
- Maintaining our own accounts and records;
- Seeking your views or comments;
- Processing a job application;
- Administering councillors' interests
- Providing a reference.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you or with an organisation that you represent.
- Where we need to comply with a legal obligation or for the performance of tasks carried out by a public authority acting in the public interest which includes the discharge of the council's statutory functions, powers and duties.

How we use sensitive personal data?

- These types of data are described in the GDPR as "Special categories of data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.
- We may process special categories of personal data relating to staff, councillors and role holders including, as appropriate:
 - information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work;
 - your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
 - in order to comply with legal requirements and obligations to third parties.
- We may process special categories of personal data in the following circumstances:
 - In limited circumstances, with your explicit written consent.
 - Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our pension scheme.
 - Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

- Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

Do we need your consent to process your sensitive personal data?

- We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law.
- In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.
- You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

- We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.
- Less commonly, we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

What is the legal basis for processing your personal data?

The council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation or for the performance of tasks carried out by a public authority acting in the public interest which includes the discharge of the council's statutory functions, powers and duties.

We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

We will also process your data in order to assist you in fulfilling your role in the council including administrative support or if processing is necessary for compliance with a legal obligation.

Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first give us your prior consent. It is possible that we will need to share your data with:

- Our agents, suppliers and contractors (for example, we use an external provider to manage our payroll and pension functions)
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC
- Staff pension providers
- Payroll services providers
- Professional advisors
- Trade unions or employee representatives

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. We will retain personal data provided to us unsolicited as part of normal correspondence for a period of 3 years plus the year the data was provided. It is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general, we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

Your rights in connection with personal data

You have the following rights with respect to your personal data: -

1. *The right to access personal data we hold on you*

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month.
- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. *The right to correct and update the personal data we hold on you*

- If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

3. *The right to have your personal data erased*

- If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase the personal data we hold.
- When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it for to comply with a legal obligation).

4. *The right to object to processing of your personal data or to restrict it to certain purposes only*

- You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. *The right to data portability*

- You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. *The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained*

- You can withdraw your consent easily by telephone, email, or by post (see Contact Details below).

7. *The right to lodge a complaint with the Information Commissioner's Office.*

- You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

When exercising any of the rights listed above, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

Transfer of Data Abroad

Personal data will not be transferred to countries or territories outside the European Economic Area ("EEA") although our website is also accessible from overseas so on occasion some personal data (for example in a newsletter) may be accessed from overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and we will place any updates on this web page <https://stocksfield-pc.gov.uk/policies-and-procedures/> .

Contact Details

Please contact us if you have any questions about this Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Stocksfield Parish Council, Stocksfield Community Association, Mount View Terrace, Stocksfield, NE43 7HL

Email: For general enquiries – dpo@stocksfield-pc.gov.uk

For subject access requests – subjectaccess@stocksfield-pc.gov.uk

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Appendix H

Stocksfield Parish Council

CONSENT FORM

Your privacy is important to us. We would like to communicate with you by email about the council and its activities but to do so we need your consent. If you wish to receive information from the Council, please fill in your name and email address below and confirm your consent by deleting 'NO' in the appropriate boxes below.

Name *(mandatory)*

Email address *(mandatory)*

Address *(optional)*

Signature *(if submitting hard copy)*

Date

You can grant consent to any or all of the purposes listed. You can find out more about how we use your data from our "Privacy Notice" which is available from our website at <https://stocksfield-pc.gov.uk/policies-and-procedures/>

I consent to Stocksfield Parish Council processing my personal data above and to communicating with me in respect of the following (please delete either **NO** to indicate **YOU CONSENT** or **YES** to indicate you **DO NOT** consent):

*** DELETE AS APPROPRIATE**

Information about funding opportunities	YES*	NO*
Requests for items for inclusion in the Council's newsletter (NE43 News)	YES*	NO*
Information in my role as a representative of a local sports club (please specify the club(s))	YES*	NO*
Electronic copies of the Council's newsletter (NE43 News)	YES*	NO*
Information in my role as a representative of another local group(s) (please specify the group(s) or organisation(s) here)	YES*	NO*
.		

You can withdraw or change your consent at any time by contacting the council office either in writing or by email:

Stocksfield Parish Council
Stocksfield Community Centre
Mount View Terrace
Stocksfield
NE43 7HL

Email: clerk@stocksfield-pc.gov.uk

Guidelines for the Retention of Records

1. Purpose of the Guidelines

These guidelines have been produced in order to:

- assist in identifying records that may be worth preserving permanently as part of the Council's archives
- prevent the premature destruction of records that need to be retained for a specified period to satisfy the legal, financial and other requirements of public administration
- provide consistency for the destruction, after specified periods, of those records not required permanently
- promote improved records management within the Council

2. The need to retain records

It is necessary to keep all records or other information that can be used as evidence, or as proof that something happened. The statutory or recommended retention periods for a range of documents and records are given in detail below.

It is not necessary to keep:

- "with compliments" slips
- catalogues and trade journals
- telephone message slips
- non-acceptance notes of invitations
- trivial electronic mail messages or notes that are not related to Parish Council business
- out-of-date distribution lists
- working papers that led to a final report
- duplicated and superseded material
- drafts or manuals
- copies of annual reports

Where a document or data item is not covered in the list (and specifically unsolicited correspondence from the general public relating to the business of the Council), the item will be destroyed or deleted after three full calendar years plus the year of its initial recording or receipt or when it is no longer necessary to retain it, whichever is the sooner.

3. Destruction of records

Wherever there is the possibility of litigation, the records and information that are likely to be relevant should not be amended or disposed of until the threat of litigation has been removed. For instance, if a child is injured at a Council-run function or in an accident in a play area, s/he can bring an action against the Parish Council at any time until s/he reaches adulthood. Similarly, an employee can make a claim for work-related injury against the Council many years after the event. For this reason, certificates of employer's liability insurance should be retained for a period of 40 years.

All paper records should be securely disposed of and treated as confidential waste. When records are destroyed, a register should be kept, giving sufficient information to identify which records have been disposed of. In deciding whether or not to destroy a record, the following questions should always be considered:

- in the case of a financial document, has the audit of that year's accounts been closed by the external auditors? If the answer is no, the document should be retained
- is the document unique in the "audit trail"? If the answer is yes, the document should be retained

- is there a statutory reason for retention? If the answer is yes, the document should be retained

4. Relevant legislation

In all matters relating to the retention of records, the Parish Council must comply with the terms of the Data Protection Act 2018, the General Data Protection Regulations, the Freedom of Information Act 2000, including the Environmental Information Regulations, and the Statute of Limitations (see the Information Commissioner's Office website at www.ico.org.uk).

5. Retention periods

Correspondence other than those excluded in section 2 above will be retained for three years plus the year of its receipt. The following additional retention periods are recommended by the Chartered Institute of Public Finance and Accountancy (CIPFA) and the Local Government Group of the Records Management Society of Great Britain

Operations area	Type of record	Retention period (years)
Accountancy	Estimate working papers	2 + current year
	Grant claim records	6
	Telephone call records	2 + current year
Contracts	Final accounts- contract under hand	6
	Final accounts- contract under seal	12
	Successful tenders	3 years after final payment
	Unsuccessful tenders	Until final payment is made to the successful tenderer, or after year of audit
Creditor Records	Copy orders	2 + current year
	Delivery notes	2 + current year
	Imprest documentation (petty cash)	2 + current year
Income Records	Correspondence	2 + current year
	Debtor accounts	2 + current year
	Receipt books	2 + current year
	Sales records	2 + current year
Miscellaneous	Computer system documentation	2 + current year
	Inventory records	6
	Land Searches	6
	Postal remittance records	2 + current year
	Stock lists	2 + current year

Misc (continued)	Vehicle logs	2 + current year
	Timesheets etc	3 + current year
Operations area	Type of record	Retention period (years)
Administration	Agendas and business papers, minutes, Council notice papers and records of proceedings	Permanent – archive - common practice
	Minute taking	Until date of confirmation of the minutes- common practice
	Civic & royal events	Permanent – archive - common practice
	Litigation	7 years after last action - common practice
	Major litigation	Archive
Employees	Disciplinary action- oral warning - written warning - final warning Records of the above warnings should be removed and destroyed when the relevant time has elapsed	6 months 12 months 18 months Warnings related to the protection and safeguarding of children should be placed on file permanently - archive
	Grievance procedures – written records	6 years after the employee has left Where a grievance is proven to be unfounded, destroy immediately or after appeal
Accounts and audit	Year end financial records	Permanent - archive after administrative use is concluded - common practice
Payroll	Employee pay records, deductions, employee tax records	7 years after the end of the financial year that the record supports - statutory
Asset monitoring and maintenance	Asset registers	7 – common practice
	Maintaining plant and equipment	7 years after sale or disposal - common practice
	Asset acquisition and disposal	6 if value is under £50,000, or 12 if value is over £50,000 - statutory
Planning	Planning applications and related documentation	1 year
Insurance	Certificates of employers' liability insurance	40 - statutory