Ettington Parish Council

Date: 16 May 2018

|  |  |
| --- | --- |
| Item 17 Appendix 4 | General Data Protection Regulations |

1. **Introduction**

This report is an update on that presented at the meeting of 14 March 2018 and seeks to:

1. Provide an update on achievement towards being compliant;
2. Seek approval for the policy and other paperwork in respect of General Data Protection Regulations
3. Seek agreement to the work plan in respect of this matter.
4. **Awareness**

To make decision makers aware of the GDPR and its impact on the organisation in order that they are aware of the impact and any likely compliance problems and the resource implications.

*Position Statement: Compliant: The report of 14 March and accompanying paperwork made Councillors aware of the changes and requirements for being compliant.*

1. **Information You Hold**

Document what personal data you hold, where it came from and who it is shared with which may necessitate an information audit.

*Position Statement: Compliant -* Audit completed

1. **Communicating Privacy Information**

Review current privacy notices and put in place a plan for making any necessary changes.

*Position Statement:* Not compliant: Privacy Notices sourced (appendix bi and bii)

Action Required: To make a resolution in respect of the Privacy Notices

1. **Individuals’ Rights**

Check procedures to ensure all rights are covered.

*Position Statement:* Not compliant . A Policy and Procedure in respect of GDPR is attached at appendix c

*Action Required: To make a resolution in respect of the Policy and Procedure*

1. **Subject Access Requests**

Update procedures and plan how to handle requests in line with the new rules:

*Position Statement:* Not compliant . A Policy and Procedure in respect of GDPR is attached at appendix c and once this is adopted and published compliance will have been achieved.

1. **Lawful Basis for Processing Personal Data**

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

*Position Statement:* Not compliant:: Refer to the workplan (appendix d)

1. **Consent**

You should review how you seek, record and manage consent and whether you need to make any changes.

*Position Statement:* Not compliant Refer to the workplan (appendix d)

1. **Children**

You should start thinking about whether you need to put sysems in place to veryify individuals’ ages and to obtain parental or guardian consent for any data processing activity.

*Position Statement:* Not compliant - refer to workplan (appendix d)

1. **Data Breaches**

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

*Position Statement:* Not compliant : Once the Policy and Procedure in respect of GDPR is adopted compliance will have been achieved.

1. **Data Protection by Design and Data Protection Impact Assessments**

GDPR makes privacy by design and express legal requirement and, in certain circumstances to undertake Privacy Impact Assessment.

*Position Statement:* Not compliant – refero to workplan (appendix e)

1. **Data Protection Officers**

As a public authority the Council must appoint a DPA who takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

NALC have issued the following update:

* + The Government has tabled an amendment to its own Data Protection Bill to **exempt** all parish and town councils and parish meetings in England and community and town councils in Wales from the requirement to appoint a Data Protection Officer (DPO) under the General Data Protection Regulation.
	+ Officials from the Department for Culture, Media and Sport have confirmed with us that all other measures will still apply, but that appointing a Data Protection Officer to support a council’s approach to data protection will be discretionary and may be regarded as good practice. The Government has tabled an amendment to its own Data Protection Bill to **exempt** all parish and town councils and parish meetings in England and community and town councils in Wales from the requirement to appoint a Data Protection Officer (DPO) under the General Data Protection Regulation.

Officials from the Department for Culture, Media and Sport have confirmed with us that all other measures will still apply, but that appointing a Data Protection Officer to support a council’s approach to data protection will be discretionary and may be regarded as good practice.

Action Required: To consider whether or not to appoint a Data Protection Officer and, if not, how the role will be covered.

1. **International**

Only relevant if the organisation carried out cross-border processing.

*Position Statement:* Not applicable

Appendix a – Audit

|  |  |  |
| --- | --- | --- |
| 1. :
 | **YOUR INFORMATION** |  |
|  | **1. Person completing questionnaire**a) Name.b) Role.c) Telephone number.d) Email. | **a) Sarah Furniss****b) Clerk****c) 01789 295827****d) epc.clerk@yahoo.com** |
|  | Data controller (e.g. name of local council or parish meeting) | Ettington Parish Council |
|  | Date you completed this questionnaire | Commenced 20 March: Completed |
| 1. :
 | **COMMUNICATING PERSONAL DATA** |  |
|  | This section relates to communications with councillors, staff and local residents (including mailing lists) general public. **a) What type of personal data does the council keep?**e.g. name, contact details such as bank details.**b) Where does the council get the personal data from?**e.g. staff, residents, other local authorities, charities and sports clubs, community groups, recruitment agencies.**c) Why does the council collect or process the data – what does the council do with the personal data?**For purposes relating to: e.g. local resident concerns, management of council facilities, services and staff, contract management, performance of statutory functions.[Please list all reasons].**d) Who does the council disclose personal data to?**E.g. the public, councillors, staff and contractors carrying out the work of the council, pension providers, HMRC, credit reference agencies, recruitment agencies, prospective employers **e) Do the council or parish meeting minutes contain personal data?****f) Does the council ever send personal data overseas and if so where to and to which organisation? This might include overseas companies providing database or email services.**e.g. do any of your suppliers use ‘cloud storage’ and if so do you know where the personal data is located?**g) Does the council collect any sensitive personal data?** see definition above.**h) If so for what reason?**e.g. for safeguarding compliance; physical or mental health data relating to staff; racial and ethnic origin relating to equal opportunities monitoring. [Please list anything else] | a)Youth Council mailing list; allotment mailing list; individual e-mail addresses, electoral roll; NP mailing list; ? MUGA bookings? b)questionnaires (NP), residents(letters, e-mail and phone calls), SDC, MUGA booking, c)resident concerns/queries; HR (eg PAYE; pension etc)allotment waiting list; allotment rental; football pitch (Ettington Rovers and Veterans); youth council; grant applications/payments; d) Councillors (forwarding resident concerns); contractors (eg in respect of Hedge Survey); HMRC; WCC; e)names of Cllrs (including SDC and WCC) – in public domain; , Community Centre rep; no member of the public names recorded now but historical minutes have names;f)Nog)noh)n/a |
| 1. :
 | **SUPPLIERS, COMPANIES, AND OTHER ORGANISATIONS THE COUNCIL CONTRACTS WITH** |  |
|  | About individuals or representatives of organisations which supply us with services such as for council repairs, or with whom we are in contact**a) Who does the council keep personal data about?**e.g. tradesman, recruitment agencies, surveyors, architects, builders, suppliers, advisers, payroll processors. [Please list any others]**b) What type of personal data does the council keep?**e.g. name, contact details, qualifications, financial details, details of certificates and diplomas, education and skills. [Please list any others]**c) Where does the council get the data from?**e.g. the individuals, suppliers. [Please list any others]**d) Why does the council collect or process the data?**e.g. council property maintenance and repairs and management of council facilities, pay and manage staff. [Please list any other reasons]. | a)Mowing contract; tree survey; tree maintenance; tender documents; hedge survey; MUGA maintenance; NP Consultant; WCC (pension provider)b) name; contact details; qualifications; membership of professional organisations; c)individual or organisationd) maintenance of playing field; pension provision;  |
| 1. :
 | **GENERAL QUESTIONS ABOUT PERSONAL DATA**  |  |
|  | 1. How does the councilstore the personal data collected?
2. Does the counciltake any steps to prevent unauthorised use of or access to personal data or against accidental loss, destruction or damage? If so, what?
3. How does the councilmanage access to data
4. What is the process involved in giving access to staff or councillors?
 | a)on laptop; back-ups (data stick and external harddrive); paper recordsb) the laptop is password protected; information is backed up monthly to both data stick (which is provided to Chairman for retention on a rotational basis) and external hard drive – neither are encrypted or locked away; PAYE data is backed up monthly; accounting package is backed up every time it is used; the laptop is kept in clerk’s home and is not locked away; paper records and kept in an unlocked filing cabinet c) As Clerk works from home she is the only person who has access to the data though, theoretically, visitors could access. d)Only the Clerk has password for computer or access to the paper records.  |
|  | 1. Do any procedures exist for e.g. correcting, deleting, restricting, personal data? If so, please provide details.
 | a)No |
|  | 1. Who has access to / is provided with the personal data (internally and externally)?
2. Is there an authorisation procedure for accessing personal data? If so, please provide details.
 | a)HMRC; WCC; Cllrs; Allotment Committee; b)no |
|  | Does the council provide a copy of all existing privacy notices? | No |
|  | So far as the council is aware, has any personal data which was gathered for one purpose been used for another purpose (e.g. communicating council news?) If so, please provide details. | No |
|  | Does the council have any policies, processes or procedures to check the accuracy of personal data? | No |
|  | 1. In the event of a data security breach occurring, does the council have in place processes or procedures to be followed?
2. What are these?
 | No |
|  | 1. If someone asks for a copy of personal data that the council holds about them, i.e. they make a ‘subject access request’, is there a procedure for handling such a request?
2. Is this procedure contained in a written document?
 | Nono |
|  | Does the council have an internal record of the consents which the council has relied upon for processing activities? e.g. to send council newsletters to residents  |  No |
|  | 1. Are cookies used on our council website?
2. Does the council provide information about the cookies used and why they are used?
3. Does the council keep a record of the consents provided by users to the cookies?
4. Does the council allow individuals to refuse to give consent?
 | 1. Need to check
2. “”
3. No
4. ?
 |
|  | Does the council have website privacy notices and privacy policies? | No |
|  | 1. What data protection training do staff (e.g. council administrator, hall bookings secretary) and councillors receive?
2. What does the training involve?
 | **a)Clerk has been on a number of training courses;****Councllors have been provided with a range of information on GDPR****B – reading and attendance at event** |
|  | 1. Does anyone in the council have responsibility for reviewing personal data for relevance, accuracy and keeping it up to date?
2. If so, how regularly are these activities carried out?
 | 1. **No**
2. **Never**
 |
|  | 1. What does the council do about archiving, retention or deletion of personal data?
2. How long is personal data kept before being destroyed or archived?
3. Who authorises destruction and archiving?
 | a)nothingb) indefinitelyc) nobody |
|  | **MONITORING** |  |
|  | 1. Please identify any monitoring of the following systems that takes place. ‘Monitoring’ includes all monitoring of systems including intercepting, blocking, recording or otherwise accessing systems whether on a full-time or occasional basis. The systems are:
2. computer networks and connections
3. CCTV and access control systems
4. communications systems (e.g. intercom, public address systems, radios, walkie-talkies)
5. remote access systems
6. email and instant messaging systems
7. telephones, voicemail, mobile phone records

 [Please list anything else]. 1. Does the council have notices, policies or procedures relevant to this monitoring?
 | 1. none

(ii)n/a(iii)n/a(iv)n/a(v)none(vi)nonb)no |

Appendix bi

**Ettington 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 (for example a name, photographs, videos, 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 (the “GDPR) 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 the Ettington Parish Council which is the data controller for your data.

**Other data controllers the council works with:**

* [e.g. other data controllers, such as local authorities
* Community groups
* Charities
* Other not for profit entities
* Contractors
* Credit reference agencies]

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the council. 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 mean 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, photographs;
* Contact details such as telephone numbers, addresses, and email addresses;
* Where they are relevant to the services provided by a 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 a council hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers, and claim numbers;
* The personal data we process may include 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.

**How we use sensitive personal data**

* We may process sensitive personal data 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.
* 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 the following circumstances:
	+ In limited circumstances, with your explicit written consent.
	+ Where we need to carry out our legal obligations.
	+ Where it is needed in the public interest.
* 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 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.

**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, telephone or using social media (e.g., Facebook, Twitter, WhatsApp);
* 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.

Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

**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 which includes the discharge of the council’s statutory functions and powers. 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 to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy

Sometimes the use of your personal data requires your consent. 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 likely that we will need to share your data with some or all of the following (but only where necessary):

* The data controllers listed above under the heading “Other data controllers the council works with”;
* Our agents, suppliers and contractors. For example, we may ask a commercial provider to publish or distribute newsletters on our behalf, or to maintain our database software;
* 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. For example, 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:

When exercising any of the rights listed below, 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.

* 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.
	1. ***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.
	1. ***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).
	1. ***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.
	1. ***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.
	1. ***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).
	1. ***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.

**Transfer of Data Abroad**

Any personal data transferred to countries or territories outside the European Economic Area (“EEA”) will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [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 [www.ettington.org](http://www.ettington.org). This Notice was last updated in xxx 2018.

**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, Sarah Furniss, 07786938072.

Email: epc.clerk@yahoo.com

Appendix bii

**Ettington 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 (the “GDPR”) 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 Ettington 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
* DBS services suppliers
* Payroll services providers
* Recruitment Agencies
* Credit reference agencies

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, photographs.
* 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, driving licence numbers, vehicle registration 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, CCTV footage, recordings of telephone conversations, 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 and referral source (e.g. agency, staff referral))
* 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.
* CCTV footage and other information obtained through electronic means such as swipecard records.
* Information about your use of our information and communications systems.

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

Please note: We need all the categories of personal data in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

* 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.
* Assessing qualifications for a particular job or task, including decisions about promotions.
* 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.
* To prevent fraud.
* To monitor your use of our information and communication systems to ensure compliance with our IT policies.
* To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
* To conduct data analytics studies to review and better understand employee retention and attrition rates.
* Equal opportunities monitoring.
* To undertake activity consistent with our statutory functions and powers including any delegated functions.
* To maintain our own accounts and records;
* To seek your views or comments;
* To process a job application;
* To administer councillors’ interests
* To provide a reference.

Our processing may also include the use of CCTV systems for monitoring purposes.

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.
* Where we need to comply with a legal obligation.

We may also use your personal data in the following situations, which are likely to be rare:

* Where we need to protect your interests (or someone else’s interests).
* Where it is needed in the public interest [or for official purposes].

**How we use sensitive personal data**

* We may process sensitive 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.
* 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 the following circumstances:
	+ In limited circumstances, with your explicit written consent.
	+ Where we need to carry out our legal obligations.
	+ 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.
* We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.]

**What is the legal basis for processing your personal data?**

Some of our processing is necessary for compliance with a legal obligation.

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 likely that we will need to share your data with:

* Our agents, suppliers and contractors. For example, we may ask a commercial provider to manage our HR/ payroll functions , or to maintain our database software;
* Other persons or organisations operating within local community.
* Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
* Staff pension providers
* Former and prospective employers
* DBS services suppliers
* Payroll services providers
* Recruitment Agencies
* Credit reference agencies
* 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. For example, 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: -

When exercising any of the rights listed below, 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.

* 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.
	1. ***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.
	1. ***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).
	1. ***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.
	1. ***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.
	1. ***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).
	1. ***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.

**Transfer of Data Abroad**

Any personal data transferred to countries or territories outside the European Economic Area (“EEA”) will only be placed on systems complying with measures giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. [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 [www.ettington.org.uk](http://www.ettington.org.uk) This Notice was last updated in xxxx 2018.

**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, Sarah Furniss, 07786938072

Email: epc.clerk@yahoo.com

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 C

Ettington Parish Council

General Data Protection Regulations Policy and Process

Date Adopted:

Due for review: Annually in May (unless legislative changes require earlier review)

1. **Purpose of the Policy and Background to the General Data Protection Regulations**
	1. This policy explains to councillors, staff and the public about GDPR.
	2. Personal data must be processed lawfully, fairly and transparently; collected for specified,

explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security.

* 1. This policy updates any previous data protection policy and procedures to include the

additional requirements of GDPR which apply in the UK from May 2018.

* 1. The Government have confirmed that despite the UK leaving the EU, GDPR will still be a

legal requirement.

* 1. This policy explains the duties and responsibilities of the council and it identifies the means

by which the council will meet its obligations.

* 1. The GDPR has six principles which are:
* **Fair Process:** Processed fairly, lawfully and in a transparent manner in relation to the data subject;
* **Collected for specific, explicit, legitimate purposes** and not processed further for purposes incompatible with those purposes
* **Adequate, relevant** and limited to what is **necessary**
* **Accurate** and, where necessary, **up to date**
* **Kept** in a form that permits identification of data subjects for **no longer than is necessary** for the purpose for which the personal data is processed
* Processed to ensure **appropriate security** including protection **against unauthorised or unlawful processing** and against **accidental loss, destruction or damage**
1. **Identifying the Roles and Minimising Risk**

2.1GDPR requires that everyone within the council must understand the implications of GDPR and that roles and duties must be assigned.

2.2 The Council is the data controller and the clerk is the Data Protection Officer(untilsuch time as there is clarity on the requirements of this role) (DPO).

2.3 It is the DPO’s duty to undertake an information audit and to manage the information collected by the council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information. This will be included in the Job Description of the clerk. Appointing the Clerk as the DPO must avoid a conflict of interests, in that the DPO should not determine the purposes or manner of processing personal data.

2.4 GDPR requires continued care by everyone within the council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the council facing a fine from the Information Commissioner’s Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as high / medium risk to the council (both financially and reputationally) and one which must be included in the Risk Management Policy of the council. Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the council undertaking training in data protection awareness.

1. **Data Breaches**
	1. One of the duties assigned to the DPO is the investigation of any breaches. Personal

data breaches should be reported to the DPO for investigation. The DPO will conduct this with the support of the council. Investigations must be undertaken within one month of the report of a breach.

3.2 The ICO will be advised of a breach within 72 hours where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPO will also have to notify those concerned directly.

3.3 It is unacceptable for employees, volunteers and members to use IT in any way that

may cause problems for the council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

1. **Privacy Notices**
	1. Being transparent and providing accessible information to individuals about how the

Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a council does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the council. The council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved. All privacy notices must be verifiable.

1. **Information Audit**

5.1 The DPO must undertake an information audit which details the personal data held,

where it came from, the purpose for holding that information and with whom the council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the council undertakes a new activity.

1. **Individuals’ Rights**

6.1 GDPR gives individuals rights with some enhancements to those rights already in

place:

• the right to be informed

• the right of access

• the right to rectification

• the right to erasure

• the right to restrict processing

• right to data portability

• the right to object

• the right not to be subject to automated decision-making including profiling.

6.2 The two enhancements of GDPR are that individuals now have a right to have their

personal data erased (sometime known as the ‘right to be forgotten’) where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.

 6.3 If a request is received to delete information, then the DPO must respond to this

request within a month. The DPO has the delegated authority from the Council to

delete information.

6.4 If a request is considered to be manifestly unfounded then the request could be

refused or a charge may apply. The charge will be as detailed in the council’s Publication Scheme (FoI). The council will be informed of such requests.

1. **Children**
	1. There is special protection for the personal data of a child. The age when a child can give their own consent, for the purpose of this policy, is 13. If the Council request consent from young people under 13, the council must obtain a parent or guardian’s consent in order to process the personal data lawfully. Consent forms for children aged 13+ must be written in language that they will understand.
2. **Summary**

The main actions arising from this policy are:

* The Council must be registered with the ICO (it is)
* A copy of this policy will be available on the Council’s website.
* The Clerk’s Contract and Job Description (if appointed as DPO) will be amended to include additional responsibilities relating to data protection.
* An information audit will be conducted and reviewed at least annually or when projects and services change.
* Privacy Notices must be issued.
* Data Protection will be included in the Council’s Risk Assessment

This policy is written with current information and advice. It will be reviewed at least annually or when further advice is issued/legislation changes.

All employees, volunteers and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

1. **Procedure in Respect of Data Subject Access Requests**
	1. Data Subject Access Requests should be addressed to the clerk in writing by post or e-mail to:

Epc.clerk@yahoo.com

Clerk to Ettington Parish Council

PO Box 6271

STRATFORD

CV37 1NX

* 1. An acknowledgement will be sent within 5 working days which may request identification verification.
	2. The request will be complied with within one month of receipt of the request.

**10 Complaint**

10.1 If the applicant/data subject is dissatisfied with the way in which his/her request has been handled then he/she has the right to make a complaint in accordance with the complaint's procedures of Ettington Parish Council.

 In addition, he/she has the right to make a complaint to the Information Commissioner at:

 Information Commissioner

 Wycliffe House

 Water Lane

 Wilmslow

 Cheshire

 SK9 5AF

**Glossary**

**Data Controller –** The person who (either alone or with others) decides what

personal information Ettington Parish Council will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for

responsible behaviour by those using personal information.

**Data Protection Officer –** The person(s) responsible for ensuring that it follows its

data protection policy and complies with the Data Protection Act 1998

**Data Subject/Service User** – The individual whose personal information is being

held or processed by Ettington Parish Council (for example: a client, an employee, a

supporter)

**‘Explicit’ consent –** is a freely given, specific and informed agreement by a Data

Subject to the processing\* of personal information\* about her/him. Explicit consent

is needed for processing sensitive\* data

\* See definition

**Notification –**  Notifying the Information Commissioner about the data processing

activities of Ettington Parish Council, as certain activities may be exempt from

notification.

**Information Commissioner –** The UK Information Commissioner responsible for

implementing and overseeing the Data Protection Act 1998.

**Processing –** Means collecting, amending, handling, storing or disclosing personal

information

**Personal Information –** Information about living individuals that enables them to be

identified – e.g. name and address. It does not apply to information about

organisations, companies and agencies but applies to named persons, such as

individual volunteers or employees within Ettington Parish Council.

**Sensitive data – means data about:**

* Racial or ethnic origin
* Political opinions
* Religious or similar beliefs
* Trade union membership
* Physical or mental health
* Sexual life
* Criminal records
* Criminal proceedings relating to a data subject’s offences

**Data Controller**

Ettington Parish Council is the Data Controller under the Act, which means that it

determines what purposes personal information held will be used for. It is also

responsible for notifying the Information Commissioner of the data it holds or is likely

to hold, and the general purposes that this data will be used for.

**Disclosure**

Ettington Parish Council may share data with other agencies such as the local

authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom

their information will be shared. There are circumstances where the law allows

Ettington

 Parish Council to disclose data (including sensitive data) without the data

subject’s consent.