Surlingham Parish Council

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

INTRODUCTION

The GDPR regulations come into force on 25 May 2018. This policy identifies how Surlingham Parish Council will meet the requirements set out in those regulations. The Council has been registered with the Information Commissioner's Office since 2017. Additional to this document is the combined Privacy Statement and Information Audit. This explains what information is held, the reason, how long it is held and who it is shared with.

This means personal data must be:

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

IDENTIFYING ROLES & MINIMISING RISK

The GDPR requires that the Council and its staff understand the implications of GDPR and that roles and duties must be assigned. The Council is the data controller (DC) and the Clerk is the data processor (DP). It is the duty of the Council to undertake an information audit and to manage the information collected by the Council, the issuing of a privacy statement, dealing with requests, complaints raised and the safe disposal of information.

The GDPR require continued care by Councillors and staff when sharing information about individuals as hard copy or electronically. A breach of the regulations could result in a fine from the Information Commissioner's Office (ICO) for the breach itself and payment of compensation to any individual(s) who are adversely affected. The handling of information is a risk to the Council (both financially and reputationally) and must be included in the Council's Annual Review of Risk Management. Potential risks will be minimised by minimising who holds protected data, and by Councillors and staff undertaking training in data protection.

DATA BREACHES
Data breaches should be reported to the DC. An investigation will be conducted by the Councillors and the Clerk. Investigations must be undertaken within one month of the report of a breach. The DC will (within 3 days of notification) advise the ICO of any breach where it is likely to result in a risk to the rights and freedoms of individuals, or result in discrimination, damage to reputation, economic loss, loss of confidentiality, or any other significant social disadvantage. Where a breach is likely to result in a substantial risk to the rights and freedoms of an individual(s) the DC will also notify those concerned directly.

INFORMATION & TECHNOLOGY – Access to the Council computer equipment is password protected and passwords are specific to the user and are not to be shared with any Councillor, employee or volunteer. No employee, volunteer or Councillor may use IT in any way that may bring the Council or individuals into disrepute. Or result in a data breach. For example, the discussion of internal Council matters on social media sites.

PRIVACY NOTICE (refer Appendix 1)
The Council will adopt a privacy notice see Appendix 1, to explain what the Council does with their personal information. The privacy notice will contain the details of the DC and the contact details of the DP, the purpose for which the information is to be used and the length of time it will be held. Individuals can, at any time, withdraw their agreement for the use of this information.

INFORMATION AUDIT (refer Appendix 1)
The DPC will 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 there is a variation in the Council's activities. The information audit review should be conducted ahead of the review of this policy and the reviews should be recorded in the minutes.

THE RIGHTS OF THE INDIVIDUAL
The GDPR confirms existing rights for individuals:

- 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.

The GDPR also give individuals the right to:

- have their personal data erased (sometime known as the 'right to be forgotten') where retention of personal data is no longer necessary for the purpose for which it was originally collected;
- data portability free of charge. Data portability refers to the ability to move, copy or transfer data easily between different computers.
- When a request is received to delete information, the DP must respond within a month. The DP has the delegated authority from the Council to delete information.
- The DP will inform the Council of such requests.

CHILDREN

There is special protection for the personal data of a child. For the purposes of these regulations the age when a child can give their own consent is 13. If the Council requires consent from a child under 13 years of age, the Council must obtain a parent or guardian's consent to process the personal data lawfully.

SUMMARY

The main actions arising from this policy are:

- The Council will be registered with the ICO.
- A copy of this policy will be available on the Surlingham village website. The policy will be considered as a core policy for the Council.
- The Clerk's Job Description will be amended to include additional responsibilities relating to data protection.
- An Information Audit will be conducted and reviewed at least annually or when activities of the Council change.
- The Privacy Notice and Information Audit See appendix 1 will be published on the Surlingham Village website.
- This policy document will be reviewed annually or earlier if further guidance is received.
- All Councillors, employees and volunteers are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.