**Seascale Parish Council**

**General Data Protection Regulation Policy**

Adopted: May 2018

To be reviewed May 2019

Purpose of the policy and background to the General Data Protection Regulation This policy explains to Councillors, staﬀ and the public about GDPR. 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. 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. The Government have conﬁrmed that despite the UK leaving the EU, GDPR will still be a legal requirement. A White Paper has been passed through the House of Commons excluding Parish and local Councils from the requirement to employ a Data Protection Officer (DPO). There is a DPO at Copeland.

This policy explains the duties and responsibilities of the Council and it identiﬁes the means by which the Council will meet its obligations. Identifying the roles and minimising risk GDPR requires that everyone within the Council must understand the implications of GDPR.

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. Some members of the Council have undertaken training in data protection awareness.

Procedures are in place to detect, report and investigate a personal data breach. The Data breaches should be reported to the clerk who will log any such breaches. The parish clerk will conduct an investigation, with the support of the Council. Investigations must be undertaken within one month of the report of a breach. ICO will be advised of a breach (within 3 days) 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 clerk will also have to notify those concerned directly.

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.

Privacy Notices 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.

Information Audit

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, will be conducted. 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. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

Individuals’ Rights

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.  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.

If a request is received to delete information, then the clerk/DPO must respond to this request within a month. The clerk/DPO has the delegated authority from the Council to delete information, with the exception of data covered by the 6-year legal retention rule.

If a request is considered to be manifestly unfounded, then the request could be refused.

Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the Council requires 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 age 13 plus, must be written in language that they will understand.

Summary The main actions arising from this policy are:

• The Council is registered with the ICO.

• A copy of this policy will be available on the Council’s website. The policy will be considered as a core policy for the Council.

• 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 on the Council’s Risk Management Policy.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

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.

Contact details:

FAO Clerk for Seascale Parish Council

c/o Seascale Library

Gosforth Road

SEASCALE CA20 1PN