Bilsington Parish Council
Ashford, KENT

www.bilsingtonpc.kentparishes.gov.uk

Parish Clerk
Peter Setterfield MILCM
Wealden House
Grand Parade
Littlestone
New Romney
Kent
TN28 8NQ
Telephone 07714300986
Email: bilsingtonclerk@gmail.com

TO: MEMBERS OF BILSINGTON PARISH COUNCIL

YOU ARE HEREBY SUMMONED to attend the Annual meeting of the PARISH COUNCIL to be held on **THURSDAY 28 SEPTEMBER 2017 at 7.30 pm** in Bilsington Village Hall, Bilsington.

Peter Setterfield

Peter Setterfield MILCM
Clerk to the Council

A G E N D A

1. **Ashford Borough Councillor's Report**
   (Time is limited to 5 minutes)

2. **Kent County Councillor's Report**
   (Time is limited to 5 minutes)

3. **Public Participation Session:**
   This provides an opportunity for members of the public to raise questions about and comment on items on the agenda. Time for this session is limited to 15 minutes (3 minutes per person).

4. **To receive apologies for absence**

5. **To receive any declarations of interest from Members**
   Members are invited to declare disclosable pecuniary interests in items on the agenda as required by the Bilsington Parish Council Code of Conduct for Members and by the Localism Act 2011.

6. **To approve the minutes of the meeting held on 27 July 2017 and 31 August 2017.**

7. **CHAIRMAN'S REPORT:**

8. **PLANNING MATTERS:**
PLANNING APPLICATION 17/1032/AS – BOURNE FARM, BOURNE ROAD, ALDINGTON – Replacement of dilapidated detached garage.

9. **FINANCE**
To approve the schedule of payments to be circulated at the meeting.

10. **NOTICE OF CONCLUSION OF AUDIT FOR THE YEAR ENDED 31 MARCH 2017**
REPORT: PKF Littlejohn LLP, the Council's External Auditor has completed its work on the Parish Council's Audit and has forwarded the certified Annual Return which is attached.

11. **VILLAGE HALL:**
An update will be given at the meeting.

12. **RESIDENT SURVEY:**
The Parish Council is asked to consider undertaking a survey of all the properties in the Parish to ascertain the views of residents which can help with the development of future plans.

13. **SPEED INDICATOR DEVICE:**
An update will be given at the meeting.

14. **GENERAL DATA PROTECTION REGULATION:**
REPORT BPC/17/06 The General Data Protection Regulation is scheduled to come into force in the UK on 25 May 2018, the provisions will be incorporated into a UK new data protection act, which will replace the Data Protection Act 1998. All Councils will need to understand their responsibilities under the new legislation.

15. **FUTURE PLANS:**
The Parish Council is asked to consider its plans for the forthcoming Remembrance Sunday and Christmas.

16. **CORRESPONDENCE:**
    a. Rural Vulnerability service – Fuel Poverty
    b. Ashford Borough Council briefing
    c. Information Commissioners Office Newsletter
    d. Rural Network Services – weekly news digest 4th September 2017

e. Rural Network Services – weekly news digest 11th September 2017
f. Rural Network Services – weekly news digest 18th September 2017
g. Kent County Council – Inside Track issue 248

17. **ANY OTHER BUSINESS:**

Bilsington Parish Council
Ashford, KENT

www.bilsingtonpc-kentparishes.gov.uk

Report Number: BPC/17/06

To: **Bilsington Parish Council**
Date: **28 September 2017**
Status: **Public Report for Decision**
From: **Parish Clerk & Responsible Financial Officer**

Subject; **GENERAL DATA PROTECTION REGULATION**

1. **SUMMARY:**
The General Data Protection Regulation is scheduled to come into force in the UK on 25 May 2018, the provisions will be incorporated into a UK new data protection act, which will replace the Data Protection act 1998. All Councils will need to understand their responsibilities under the new legislation.

2. **REASON FOR RECOMMENDATIONS:**
The Parish Council is registered with the Information Commissioners Office who oversee Data Protection Regulations and can inspect the Council's records to ensure compliance. The Parish Council therefore needs to be able to demonstrate that it is following the correct procedures at all times, as any breaches may give rise to fines being imposed.

3. **RECOMMENDATIONS:**
   1. **To receive and note Report BPC/17/06.**
   2. **To receive and adopt the Information Governance Framework Policy.**
   3. **To receive and adopt the Information Security Incident Management Policy**
   4. **To receive and adopt the Information Risk Policy**
   5. **To receive and adopt the Privacy Impact Assessment Policy**
   6. **To receive and adopt the Subject Access Policy**
   7. **To receive and adopt the Data Sharing Policy**

4. **INTRODUCTION**
The Information Commissioner's Office undertook a survey of Councils to ascertain the level of compliance with the Data Protection Act and the policies in place. The survey identified the ten basic policies that need to be in place the results showed that the majority of Councils had a lot of work to do to become compliant.

A review of the Council's policies has identified that Bilsington has in fact only four of the ten policies in place. Attached to this report are the necessary policies to redress the shortcomings.

5. SUMMARY:

The Information Commissioners Office is releasing information updates on a regular basis. At this stage it is clear that there is a lot of work required to meet the new Regulation it is already known that a full audit of the data held by the Council, both electronic and hard copy is required.

6. CONTACT OFFICER AND BACKGROUND DOCUMENTS

If you have any queries about this report please contact The Responsible Financial Officer of the Council

Tel 07714300986 or email bilsingtonclerk@gmail.com

Background Documents:

None.

Bilsington Parish Council

INFORMATION GOVERNANCE POLICY

1. Introduction

1. Bilsington Parish Council recognises information as an important asset in the provision and effective management of services and resources. It is of paramount importance therefore that information is processed within a framework designed to support and enable appropriate Information Governance.
2. Information Governance is a set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information at an organisational level, and designed to support regulatory, legal, risk, environmental and operational requirements.

2. Aim

1. The aim of this policy is to outline an information governance framework that ensures Bilsington Parish Council:
   i. Treats information as a valuable asset;
   ii. Maintains compliance with relevant UK and European Union legislation, for example the Data Protection Act 1998;
   iii. Has in place policies, procedures and guidelines designed to support appropriate information handling and management.
   iv. Demonstrates organisational commitment by setting out roles and responsibilities of staff;
   v. Has in place appropriately trained Information Governance staff available to provide advice and support to the Council.

3. Scope

1. This policy applies to:
   i. All information, regardless of format, processed by Bilsington Parish Council;
   ii. All information systems operated or managed by Bilsington Parish Council;
   iii. Any individual processing information held by Bilsington Parish Council;
   iv. Any individual requiring access to information held by Bilsington Parish Council.

4. Objectives

1. This policy requires a Bilsington Parish Council Information Governance framework which is multi-disciplined in its approach and seeks to achieve the following objectives:
   i. Obtains information fairly and lawfully;
   ii. Records information accurately and reliably;
   iii. Holds information securely;
   iv. Shares information appropriately and legitimately;
   v. Supports the delivery of services.

5. The Information Governance Framework

1. When processing information there are a number of legal obligations placed upon Bilsington Parish Council which will inform the way information governance is applied. In addition there are a variety of standards, principles and best practices which have been adopted to improve the way Bilsington Parish Council handles information. Bilsington Parish Council shall seek to achieve and maintain compliance with:
   i. The Data Protection Act 1998;

ii. The Human Rights Act 1998;
iii. Freedom of Information Act 2000;
iv. Local Government Act 1972;
v. Information security management systems – ISO/IEC 27001:2013.

2. To further support the Information Governance Framework Bilsington Parish Council shall develop and maintain a number of local policies which support and embed information processes. The key policies are:
    2. Data Protection Policy
    3. Freedom of Information Policy
    4. Information haring Policy
    5. Records Management Policy
    6. Information Security Policy

6. Compliance

1. All Council employees have a contractual responsibility to be aware of and conform to the Council's values, rules, policies and procedures. Breaches of policy may lead to the employee going through the Council's disciplinary policy and procedure.
2. Individuals who are not Council employees and who fail to comply with the Council's policies may have their access to Council information revoked and such action could have an impact on contracts with third party organisations.

7. Policy Review

1. This policy will be reviewed on an annual basis.

Bilsington Parish Council.

Information Security Incident Management Policy

1. Introduction

Bilsington Parish Council is responsible for the security and integrity of all data it holds. The Council must protect this data using all means necessary by ensuring at all times that any incident which could cause damage to the Council's assets and reputation is prevented and/or minimised. There are many types of incidents which could affect security;

- A computer security incident is an event affecting adversely the processing of computer usage. This includes:
    - Loss of confidentiality of information
    - Compromise of integrity of information
    - Denial of service
    - Unauthorised access to systems
    - Misuse of systems or information
    - Theft and damage to systems
    - Virus attacks
    - Intrusion by humans
- Other incidents include;
    - Missing correspondence
    - Exposure of uncollected printouts
    - Misplaced or missing media
    - Inadvertently relaying passwords
    - Loss of mobile phones and portable devices.

Ensuring efficient reporting and management of security incidents will help reduce and in many cases, prevent incidents occurring.

More detailed information on the type and scope of security incidents is provided in the Policy Statement section of this policy.

2. Purpose

The management of security incidents described in this policy require the Council to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incidents
- Detail procedures in place for reporting and processing of incidents
- Provide guidance

3. Scope

This policy applies to:

- Council employees, elected members, partner agencies, contractors, volunteers and vendors

- All Council personnel and systems (including software) dealing with the storing, retrieval and accessing of data.

4. Policy Statement

The Council has a clear incident reporting mechanism in place which details the procedures for the identifying, reporting and recording of security incidents. By continually updating and informing Council employees, elected members, partner agencies, contractors, volunteers and vendors of the importance of the identification, reporting and action required to address incidents, the Council can continue to be pro-active in addressing these incidents as and when they occur.

All Council employees, elected members, partner agencies, contractors, volunteers and vendors are required to report all incidents – including potential or suspected incidents, as soon as possible via the Council's Incident Reporting procedures.

The types of incidents which this policy addresses include but is not limited to:

Computers left unlocked when unattended

Users of Council computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All Council employees, elected members, partner agencies, contractors, volunteers and vendors need to ensure that they lock their computers appropriately – this must be done despite the fact that Council computers are configured to automatically lock after 10 minutes of idle time.

Discovery of an unlocked computer which is unattended must be reported via the Council's Incident Reporting procedures.

Password disclosures

Unique ID's and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others – regardless of trust. If an individual needs access to data or a system, they must go through the correct procedure for authorisation.

Virus warnings/alerts

All computers across the Council have antivirus (including Anti-spyware/Malware). For the most part, the interaction between the computer and antivirus software will go unnoticed by users of the computer. On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to Council data. The warning message may indicate that the antivirus software may not be able to rectify the problem and so must be reported as soon as possible.

Media loss

Use of portable media such as CD/DVD, USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorised access. Any unauthorised user of a portable device (including portable media) who has misplaced or suspects damage, theft whether intentional or accidental must report it immediately through the Council's Incident Reporting procedures.

Data loss/ disclosure

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorised recipient (such as the use of email to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the Council's website and identified as inaccurate or inappropriate
- Conversationally – information disclosed during conversation
- Press or media – unauthorised disclosure by employees or an ill-advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Unlocked and uncollected print-outs from Multi-Function devices (MFDs)
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All Council employees, elected members, partner agencies, contractors, volunteers and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of Council data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately using the Council's Incident Reporting procedures.

Personal information abuse

All person identifiable information – i.e. information which can identify an individual such as home address, bank details etc. must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.

Any abuse/misuse of such person identifiable information must be reported through the Council's Incident Reporting procedures.

Physical security

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices which have been designated specifically as areas where secure information is located or stored must have a method of physically securing access to the room – e.g. a combination key lock mechanism. Lower/floor level windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data.

Logical Security / Access Controls

Controlling, managing and restricting access to the Council's databases and applications is an essential part of Information Security. It is necessary to ensure that only authorised employees can gain access to information which is processed and maintained electronically.

Missing correspondence

Data or information which has been sent either electronically or physically which cannot be accounted for e.g. not arrived at the intended destination via physical post, sent electronically, sent for printing but no print output retrieved etc., must be reported through the Council's Incident Reporting procedures.

Found correspondence/media

Data stored on any storage media or physically printed information which has been found in a place other than a secure location or a place where the security and integrity of the data/information could be compromised by unauthorised viewing and/or access e.g. unlocked printouts, discarded CD (media), must be reported vis the Council's Incident Reporting procedures.

Loss or theft of IT/information

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinets, etc., or which is known/or suspected to have been stolen needs to be reported immediately through the Council's Incident Reporting procedures.

5. Responsibilities

It is the responsibility for all Council employees, elected members, partner agencies, contractors, volunteers and vendors who undertake work for the Council, on or off the premises to be proactive in the reporting of security incidents. The Council's Incident Reporting procedures are in place to prevent and minimise the risk of damage to the integrity and security of Council data and information.

It is also a responsibility of all individuals and handlers of Council data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed.

6. **Compliance with legal and contractual obligations**.

The Data Protection Act (1998) requires that personal data be kept secure against unauthorised access or disclosure.

The Computer Misuse Act (1990) covers unauthorised access to computer systems.

7. Breaches of Policy

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to Council assets, including IT equipment and information, or conduct which is in breach of the Council's security procedures and policies.

All Council employees, elected members, partner agencies, contracts, volunteers and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, volunteers, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant

frameworks in place. In the case of an employee, infringements will be investigated under the disciplinary procedure and progressed as appropriate.

8. Incident Management

All parties dealing with security incidents shall undertake to:

- Analyse and establish the cause of the incident and take any necessary steps to prevent recurrence
- Report to all affected parties and maintain communication and confidentiality throughout investigation of the incident
- Identify problems caused as a result of the incident and to prevent or reduce further impact
- Contact 3rd parties to resolve errors/faults in software and to liaise with the relevant parties to ensure contractual agreements and legal requirements are maintained and to minimise potential disruption to other Council systems and services
- Ensure all systems logs and records are securely maintained and available to authorised personnel when required
- Ensure only authorised personnel have access to systems and data
- Ensure all documentation and notes are accurately maintained and recorded
- Ensure all authorised corrective and preventative measures are implemented and monitored for effectiveness

Where appropriate, incidents will be presented to the full Council via the agenda and will be included on the Corrective and Preventative Action log.

All incidents logged shall have all the details of the incident recorded – including any action/resolution, links or connections to other known incidents, incidents which were initially resolved but have recurred will be reopened or a new incident referencing the previous one will be created.

During the course of incident investigations, hardware, logs and records may be analysed by the Council's internal Audit function. Information and data may be gathered as evidence to support possible disciplinary or legal action. It is essential during the course of these investigations that confidentiality is maintained at all times.

Bilsington Parish Council

Information Risk Management Policy

1. **Aim**
    1. The aim of this policy is to set out Bilsington Parish Council's approach to information risk management.
2. **The Purpose of Information Risk Management**
    1. Information Risk Management is a key element of information assurance and the corporate governance of an organisation. It ensures risks are considered against organisational benefits and assists in exploiting information opportunities whilst maintaining confidence and reassurance that risks are appropriately managed.
3. **Identifying Information Risk**
    1. Bilsington Parish Council uses various internal and external sources to identify information risks including:
        1. Local threat assessment;
        2. Monitoring compliance with Information Security Management System;
        3. National advice and guidance;
        4. Security incident reporting;
        5. Technical and procedural failures;
        6. Change management;
        7. Information Technology Health Checks / Penetration testing;
        8. External statutory and regulatory obligations;
        9. Policy exceptions.
4. **Assessing Risk**
    1. A qualitative risk assessment, based on the corporate risk approach is used to assess the probability of an event happening and the impact should it happen.
    2. Confidentiality, integrity or availability of the assets form part of the assessment.
    3. A scale of 1 – 4 for likelihood and impact is used in line with the corporate risk model.
5. **Treatment of Information Risk**
    1. Bilsington Parish Council address information risk using four key aspects of Information Risk Management internal control:
        1. Tolerate – the decision on retaining the risk without further action.
        2. Treat – the decision to introduce, remove or alter controls so that the residual risk can be reassessed as being acceptable. This must be achieved through the following actions:
            a. Preventative – stop undesirable events happening e.g. limiting action to an authorised person;
            b. Corrective – restore normality after the occurrence of undesirable events e.g. business continuity planning;
            c. Directive – encourage desired behaviour or outcomes e.g. training staff; and
            d. Detective – detect the occurrence of undesirable events e.g. audit and monitoring.

3. Transfer – the decision to transfer the risk to another party in order to manage the risk more effectively. Reputational risk cannot be transferred.
4. Terminate – the decision to avoid the risk completely by withdrawing from a planned or existing activity or set of activities.

6. Monitoring Information Risk

1. Risks and their factors will be monitored and reviewed:
    1. Context – identifying changes to underlying assumptions or new factors.
    2. Controls – ensuring the controls for risks do not become less effective or irrelevant.
    3. Treatments – ensuring risk treatments are appropriately implemented and maintained.

7. Recording Information Risk

1. Information Risk Register

1. An Information Risk Register will be maintained and will act as a central repository for high level information risks. The Information Risk Register will be available at all times to those involved in the risk process.

2. Risk Balance Case

1. A Risk Balance Case approach has been adopted to capture information risks created as a result of policy exceptions

3. Information Security Management System Risk Register

1. A risk register holding risks specific to the management of the information security management system and related controls will be maintained.

8. Shared Risk

1. Bilsington Parish Council recognise that ownership of information risk can be shared and the impact can therefore be external to Bilsington Parish Council, for example through partnership working.
2. Bilsington Parish Council will work with its partners to ensure risks are managed and communicated to ensure organisations can discharge their responsibilities appropriately.

9. Risk Appetite Levels

1. Taking into account the internal and external factors the risk appetite for information risks is **Cautious.**
2. The following table presents the corporate risk appetite levels.

Appetite Levels	Description
Averse	Preference for safe business delivery options that have a low degree of inherent risk and only a potential for limited reward. Low risk options taken to minimise exposure – reluctant to take action given uncertainty – highly influenced by experience.
Cautious	Preference for safe delivery options that have a medium degree of residual risk and may only have limited potential for reward.

	'willing to take risks but prefer to take the 'safe delivery option' – minimising the exposure with tight corporate controls over change'
Creative and Aware	Wiling to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing a good level of reward. 'no surprises – well measure risk taking – willing to take risk with a degree of uncertainty – recognising things will go wrong – learn from mistakes'
Hungry	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk. Recognise highly developed decision making – will mean that not all risks are known – take action when uncertain of results or with uncertain info – willing to accept significant loss (money/reputation) for higher potential reward'

Bilsington Parish Council

What the Information Commissioners Office means by Privacy Impact Assessment

Privacy Impact Assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective Privacy Impact Assessment will be used throughout the development and implementation of a project, using existing project management processes. A Privacy Impact Assessment enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

The Information Commissioners Office uses the term project in a broad and flexible way – it means any plan or proposal in an organisation, and does not need to meet an organisation's formal or technical definition of a project, for example set out in a project management methodology.

Privacy Impact Assessments are often applied to new projects, because this allows greater scope for influencing how the project will be implemented. A Privacy Impact Assessment can also be useful when an organisation is planning changes to an existing system, but the organisation needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system.

The purpose of the Privacy Impact Assessment is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

These can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy.

Each organisation will be best placed to determine how it considers the issue of privacy risks. The steps in this code can be applied to a wide range of business processes. The Information Commissioners Office has designed its Privacy Impact Assessment methodology to be as flexible as possible so that it can be integrated with an organisation's existing ways of working.

Conducting a Privacy Impact Assessment does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two forms, and these can be subject to different types of intrusion:

- Physical privacy – the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of

collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages.

This code is concerned primarily with informational privacy, but an organisation can use Privacy Impact Assessments to assess what they think are the most relevant aspects of privacy.

Privacy risk is the risk of harm arising though an intrusion into privacy. This code is concerned primarily with minimising the risk of informational privacy – the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient or out of date;
- Excessive or irrelevant;
- Kept far too long;
- Disclosed to those who the person it is about does not want to have it;
- Used in ways that are unacceptable to or unexpected by the person it is about; or
- Not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a Privacy Impact assessment should be a minimisation of privacy risk. An organisation will need to develop an understanding of how it will approach the broad topics of privacy and privacy risks. There is not a single set of features which will be relevant to all organisations and all types of project – a central government department planning a national crime prevention strategy will have a different set of issues to consider to an app developer programming a game which collects some information about users.

Understanding privacy risk in this context does though require an understanding of the relationship between an individual and an organisation. Factors that can have a bearing on this include:

- Reasonable expectations of how the activity of individuals will be monitored.
- Reasonable expectations of the level of interaction between an individual and an organisation.
- The level of understanding of how and why particular decisions are made about people.

Public bodies need to be aware of their obligations under the Human Rights Act. Article 8 of the European Convention on Human Rights guarantees a right to respect for

private life which can only be interfered with when it is necessary to meet a legitimate social need. Organisations which are subject to the Human Rights Act can use a Privacy Impact Assessment to help ensure that any actions that interfere with the right to private life are necessary and proportionate.

The benefits of a Privacy Impact Assessment

Conducting a Privacy Impact Assessment is not a legal requirement of the Data Protection Act. The Information Commissioners Office promotes Privacy Impact Assessments as a tool which will help organisations to comply with their Data Protection Act obligations, as well as bringing further benefits. Carrying out an effective Privacy Impact Assessment should benefit the people affected by a project and also the organisation carrying out the project.

Whilst a Privacy Impact Assessment is not a legal requirement the Information Commissioners Office may often ask an organisation whether they have carried out a Privacy Impact Assessment. It is often the most effective way to demonstrate to the Information Commissioners Office how personal data processing complies with the Data Protection Act.

The first benefit to individuals will be that they can be reassured that the organisations which use their information have followed best practice. A project which has been subject to a Privacy Impact Assessment should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A second benefit to individuals is that a Privacy Impact Assessment should improve transparency and make it easier for them to understand how and why their information is being used.

Organisations that conduct effective Privacy Impact Assessments should also benefit. The process of conducting the assessment will improve how they use information which impacts on individual privacy. This should in turn reduce the likelihood of the organisation failing to meet its legal obligations under the Data Protection act and of a breach of the legislation occurring.

Conducting and publicising a Privacy Impact Assessment will help an organisation to build trust with the people using their services. The actions taken during and after the Privacy Impact Assessment process can improve an organisation’s understanding of their customers.

There can be financial benefits to conducting a Privacy Impact Assessment. Identifying a problem early will generally require a simpler and less costly solution. A Privacy Impact Assessment can also reduce the ongoing costs of a project by minimising the amount of information being collected or used where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of Privacy Impact Assessments will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of the project.

Projects which might require a Privacy Impact Assessment.

The core principles of Privacy Impact Assessments can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

Privacy Impact Assessment terminology often refers to a project as the subject of a Privacy Impact Assessment and this should be widely construed. A Privacy Impact Assessment is suitable for a variety of situations:

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system (for example adding Automatic number plate recognition capabilities to existing CCTV).
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection of use of information, or through surveillance or other monitoring.

A Privacy Impact Assessment should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that Privacy Impact Assessments are more likely to be of use when applied to new projects or revisions of existing projects. Conducting a Privacy Impact Assessment of an existing project is less likely to make a positive difference unless it is possible for necessary changes to be implemented.

Organisations should develop the capability to identify the need for a Privacy Impact Assessment at an early stage and should consider building this into their project management or other business processes.

Responsibility for conducting a Privacy Impact Assessment.

Each organisation can decide who is best placed to coordinate and carry out the Privacy Impact Assessment process. Large organisations are more likely to have a dedicated Data Protection Officer. A Data Protection Officer is naturally well-placed to have a significant role in a Privacy Impact Assessment, and may also be able to design a set of Privacy Impact Assessment tools which mirror an organisation's existing processes. They may also maintain a log of all Privacy Impact Assessments carried out in the organisation.

Not all organisations have their own Data Protection Officer, or it may be difficult for a Data Protection Officer to conduct all the Privacy Impact Assessments – the general approach to Privacy Impact Assessments is also intended for use by non-experts. Project, risk or other managers without specialist data protection knowledge should be able to use the screening questions in Annex one to help them focus on privacy issues. An effective Privacy Impact Assessment will include some involvement from various people in an organisation, who will each be able to identify different privacy risks and solutions.

Step one: Identify the need for a Privacy Impact assessment

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a Privacy Impact Assessment was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted, internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

Consultation can be used at any stage of the Privacy Impact Assessment process.

Step three: identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale Privacy Impact Assessments might record this information on a more formal risk register.

Annex three can be used to help identify the Data Protection Act related compliance risks

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: sign off and record the Privacy Impact Assessment outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the Privacy Impact Assessment outcomes back into the project plan

Who is responsible for integrating the Privacy Impact Assessment outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Annex one

Privacy impact assessment screening questions

These questions are intended to help organisations decide whether a Privacy Impact Assessment is necessary. Answering ‘yes’ to any of these questions is an indication that a Privacy Impact Assessment would be a useful exercise. You can expand on your answers as the project develops if you need to.

Wil the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Will the project require you to contact individuals in ways which they may find intrusive?

Annex two

Linking the Privacy Impact Assessment to the data protection principles

Answering these questions during the Privacy Impact Assessment process will help you to identify where there is a risk that the project will fail to comply with the Data Protection Act or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) **At least one of the conditions in Schedule 2 is met, and**
b) **In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**

Have you identified the purpose of the project?

How will individuals be told about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the European Economic Area?

If you will be making transfers, how will you ensure that the data is adequately protected?

Bilsington Parish Council

Subject Access Requests Policy

Managing everyone's right of access to their personal data

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how? For each point further down the page.

What must 1 do?

1. ***MUST:*** we must correctly **identify** whether a request has been made under the Data Protection Act.
2. ***MUST:*** any employee who receives a request to locate and supply information relating to a Subject Access Request must make a full exhaustive search of the records to which they have access.
3. ***MUST:*** all the information that has been requested must be **provided** unless an exemption can be applied.
4. ***MUST:*** we must **respond** within 40 calendar days after accepting the request as valid.
5. ***MUST:*** Subject Access Requests must be undertaken **free of charge** to the requestor
6. ***MUST:*** log the **receipt and fulfilment** of all requests received by Bilsington Parish Council from a data subject to see his or her personal information. They must also respond to such requests on behalf of People Operations teams where the information is held in closed case files.
7. ***MUST:*** where a requestor is not satisfied with a response to a Subject Access Request, Bilsington Parish Council must manage this as a **complaint.**

Why must I do it?

1. So it can be correctly identified as a Subject Access Request and processed accordingly
2. In order to manage the request under the current legislation
3. The law requires that disclosure must be based on reviewing all personal data relevant to the request
4. The act requires a full disclosure to be made unless there is a legal reason for withholding all or some of the information
5. This is a statutory requirement
6. Although the Act allows us to charge up to £10 for processing requests, Bilsington Parish Council considers collecting this charge to be viewed as potentially obstructive to people making such requests, and due to administrative costs in collecting and processing the payment would result in negligible cost benefit to Bilsington Parish Council.
7. Bilsington Parish Council must be able to evidence its performance under the act to the Information Commissioners Office.
8. The act requires an internal complaints process to be in place before a complaint may be escalated to the Information Commissioners Office.

How must I do it?

1. As defined by section 7 of the Data Protection Act. We must ensure a request has been received in writing where a data subject is asking for sufficiently well-defined personal data held by Bilsington Parish Council relating to themselves. The Act permits and encourages us to clarify with the requestor what

information they need. They must supply their address and valid evidence to prove their identity. Bilsington Parish Council accepts the following forms of identification (* these documents must be dated in the past 12 months, + these documents must be dated in the past 3 months)

a. Current UK/EEA Passport
b. UK Photocard Driving Licence (Full or Provisional)
c. Firearms Licence / Shotgun certificate
d. EEA National Identity Card
e. Full UK Paper Driving Licence
f. State Benefits Entitlement Document*
g. State Pension Entitlement Document*
h. HMRC Tax Credit Document*
i. Local Authority Benefit Document*
j. State/ Local Authority Educational Grant Document*
k. HMRC Tax Notification Document
l. Disabled Driver's pass
m. Financial statement issued by bank, building society or credit card company+
n. Judiciary document such as a Notice of hearing, Summons or Court Order
o. Utility bill for supply of gas, electric, water or telephone landline+
p. Most recent mortgage statement
q. Most recent Council Tax Bill/Demand or statement
r. Current Council Rent Card
s. Current Council Tenancy Agreement
t. Building Society Passbook which shows a transaction in the last 3 months and your address

2. Depending on the degree to which information is organised and structured, you will need to 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), tape recordings, paper records in relevant filing systems etc which your area is responsible for or owns.
3. You must not withhold information because you believe it will be misunderstood; instead, you should provide an explanation with the information. You must provide the information in an "intelligible form", which includes giving an explanation of any codes, acronyms and complex terms. The information must be supplied in a permanent form except where the person agrees or where it is impossible or would involve undue effort. You may be able to agree with the requester that they will view the information on screen or inspect files on our premises. You must redact any exempt information from the released documents and explain why that information is being withheld.
4. A database is maintained allowing Bilsington Parish Council to report on the volume of requests and compliance against the statutory timescale.
5. When responding to a complaint, we must advise the requestor that they may complain to the Information Commissioners Office if they remain unhappy with the outcome.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, check to see if there is a current Exception to Policy request available.

Bilsington Parish Council.

Information Sharing Policy

1. Aim

1.1. The aim of this policy is to support and facilitate effective and lawful sharing of information between Bilsington Parish Council and third parties within the public, private and third sector.

1.2. It promotes the accurate, timely, and secure sharing of information in a manner consistent with Bilsington Parish Council's legislative responsibilities defined by the Data Protection Act 1998 as well as sector led legislation and guidance.

2. Introduction

2.1. Effective sharing of information across organisational and professional boundaries plays a crucial role in providing efficient services to the public across a range of sectors.

2.2. As Bilsington Parish Council shares large amounts of personal data with defined third parties in order to maximise public service delivery, and to meet its statutory responsibilities, it is important to maintain trust in the way this is achieved by demonstrating that it is done so in a lawful, responsible and secure manner.

3. Types of information sharing

3.1. Information sharing in the context of this policy means the sharing of personal data from one or more organisations to another. The two main types of information sharing are:

3.1.1. Systematic, routine, data sharing where the same data sets are shared between the same organisations for an established and agreed purpose; and

3.1.2. Exceptional, one off decisions, to share data for any of a range of appropriate and agreed purposes.

4. Personal Data and Sensitive Personal Data

4.1. In most circumstances it will be reasonably straightforward to determine whether the information is personal data and therefore regulated by the Data Protection Act.

4.2. If a living individual can be identified from the data, or, from the data and other information in Bilsington Parish Council's possession, or likely to come into Bilsington Parish Council's possession and it relates to an identifiable living individual, whether in personal or family life, business or profession, it is personal data.

4.3. Sensitive personal data means personal data consisting of:

4.3.1. The racial or ethnic origin of the data subject.

4.3.2. His/her political opinions;

4.3.3. His/her religious beliefs or other beliefs of a similar nature;

4.3.4. Whether he/she is a member of a trade union;

4.3.5. His/her physical or mental health or condition;

4.3.6. His/her sexual life;

4.3.7. The commission or alleged commission by him/her of any offence; or

4.3.8. Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

5. Data Protection Act 1998

5.1. The Data Protection Act 1998 applies to personal data and gives individuals a number of important rights to ensure that personal information covered by the Act is processed lawfully.

5.2. It regulates the manner in which such information can be collected, used and stored, and so is of prime importance in the context of information sharing.

5.3. Key principles in the Data Protection Act 1998 state that personal information must:

5.3.1. Be processed fairly and lawfully;

5.3.2. Be obtained for a specified and lawful purpose and not processed in a manner incompatible with that purpose;

5.3.3. Be adequate, relevant and not excessive for the purpose;

5.3.4. Be accurate and, where necessary kept up to date;

5.3.5. Not kept longer as is necessary;

5.3.6. Be processed in accordance with the rights of the data subject;

5.3.7. Be subject to appropriate technical and organisational measures designed to prevent unauthorised/unlawful processing and accidental loss, destruction or damage;

5.3.8. Not be transferred outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

6. Before You Decide to Share Personal Data

6.1. Before sharing personal data you must identify the objective of sharing and carefully consider the following factors:

6.1.1. What is the sharing meant to achieve?

6.1.2. Could the objective be achieved without sharing the data or by anonymising it?

6.1.3. What is the legal basis for sharing the information?

6.1.4. What information needs to be shared and who requires access?

6.1.5. How and when should it be shared?

6.1.6. How can we check the sharing is achieving its objectives?

6.1.7. What risk does the data sharing pose?

6.1.8. How will any shared data be kept up to date?

7. Lawful Sharing

7.1. You must ensure personal data is only shared where it is fair and lawful. The first principle of the Data Protection Act 1998 requires that you must satisfy one or more conditions in order to legitimise the processing i.e. sharing of personal data.

7.2. Sharing involving sensitive personal data can be undertaken only when a further more exacting condition has been satisfied in accordance with the first data protection principle.

7.3. Conditions for sharing are set out at Annex A to this policy.

8. Fairness and Transparency

8.1. You must ensure that personal data is shared fairly and in a way that is reasonable. People should generally be aware who you are sharing their personal data with and what it is being used for.

8.2. Bilsington Parish Council will maintain a privacy notice in line with the Information Commissioners Office Code of Practice.

8.3. To support a transparent approach you should consider proactively communicating a privacy notice, for example when sharing sensitive personal data or where the sharing of data will have a significant effect on the individual.

8.4. You must work together with partner organisations to ensure that the individuals concerned know who has, or will have, their data and what it is being used for.

9. Individual Rights

9.1. The Data Protection Act gives individuals certain rights over their personal data. These include:

9.1.1. The right to access personal data held about them;

9.1.2. The right to know how their data is being used; and

9.1.3. The right to object to the way their data is being used.

9.2. An information sharing initiative must take into consideration individual rights and have in place mechanisms to support individuals.

9.3. If a significant number of objections, negative comments or other expressions of concern are received regarding a particular information sharing process, a review of the data sharing in question will be carried out.

10. Security of information

10.1. Information sharing partners will have varying degrees of technical, physical and procedural security controls in place.

10.2. It is important therefore to ensure consistency in approach by agreeing common minimum standards which can be achieved by all partners and which provided appropriate assurance when sharing personal data.

11. Privacy Impact Assessment

11.1. Privacy Impact Assessments are intended as a means for Bilsington Parish Council to identify and minimise the privacy risks concerned with sharing information and support our requirement to comply with data protection law.

12. Information Sharing Agreements

12.1. You must document instances of systematic information sharing within information sharing agreements. These must include:

12.1.1. The purpose, or purposes, of the sharing:

12.1.2. The potential recipients or types of recipient and the circumstances in which they will have access.

12.1.3. The data to be shared;

12.1.4. The process for sharing;

12.1.5. Data quality – accuracy, relevance, usability, etc.

12.1.6. Data security;

12.1.7. Retention of shared data;

12.1.8. Individuals' rights – procedures for dealing with access requests, queries and complaints.

13. Ad hoc or 'one off' sharing

13.1. It may not always be possible to document the sharing of information in an emergency or time dependent situation and sharing may depend primarily on the exercise of professional judgement.

13.2. Where this is the case you must make a record as soon as possible, detailing the circumstances, what information was shared and explaining why the disclosure took place.

13.3. In the event that ad hoc instances of information sharing become a regular occurrence, it must be considered whether it is necessary to amend an existing information sharing agreement to reflect this change or whether a separate information sharing agreement is required.

14. Information Requests and Disclosures

14.1. Alongside business as usual requests, which can usually be dealt with quickly and easily in the normal course of business, there are a number of different types of information request that staff are likely to encounter while conducting Council business.

Annex A – Conditions for Processing

Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary; in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract)
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

If the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle.

These other conditions are as follows:

- The individual whom the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of the individual (in a case where the individual's consent cannot be given or reasonably obtained), or another person (in a case where the individual's consent has been unreasonably withheld)
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings, for obtaining legal advice, or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.