General Data Protection Policy

Document Control			
Policy Owner	Head of IT, Barry O'Hagan		
Policy Author	Head of IT, Barry O'Hagan		
Version	1.0		
Consultation	Senior Management Team Yes / No Trade Unions Yes / No		
Equality Screened by	Yes/ No	**Date**	
Equality Impact Assessment	Yes or No or N/A	**Date**	
Good Relations	Yes or No or N/A		
Approved By	(Policy & Resources)	**Date**	
Adopted By	Council	**Date**	
Review Date		**By Whom**	
Circulation	Councillors, Staff, Intranet		
Document & legislation Linkages and	Internet policy Mobile Phone Policy Email and Instant Messaging Policy The Privacy and Electronic Communications Regulations (PECR) Regulation of Investigatory Powers Act 2000 Lawful Business Practice Regulations,.		

CONTENTS PAGE (to be finalised last)

1.0 INTRODUCTION

The new Data Protection Act 2018 (DPA) replaces the old data protection legislation and came into force on 25th May 2018.

The 2018 Act modernises data protection laws in the UK to make them fit-for-purpose for our increasingly digital economy and society. As part of this, the 2018 Act applies the EU's GDPR standards, by having strong data protection laws and appropriate safeguards.

The legislation is ensuring that modern, innovative uses of data can continue. At the same time, it has strengthened the controls and protection individuals have over their data.

The data protection principles set out the main responsibilities for the Council.
The principles are similar to those in the old DPA, with added detail at certain points and a new accountability requiring Council demonstrates and documents how we comply with the principles – for example by documenting the decisions you take about a processing activity.

Good Data Protection practice is not just a matter of legal compliance and ticking the boxes. Data Protection is about taking care of people and respecting their privacy. Poor practice or a serious breach could not only harm individuals but would also have a serious effect on the reputation, employees and the financials of the Council.

2.0 POLICY AIM & OBJECTIVES

2.1 **Policy Aim**:

i. To provide assurance to our employees and public that we seek to protect the information we hold and used it for legitimate purposes.

ii. To replace the existing Policy and ensure Council meets the requirements of the General Data Protection Act 2018

iii. To ensure that all appropriate staff are properly trained, kept fully informed of their obligations under the Data Protection Act 2018, and that they are aware of their personal data protection liabilities, setting out the standards expected by the Council in relation to processing of personal data and safeguarding individuals' rights and freedoms.

2.2 **Policy Objectives:**

To ensure the protection of personal and sensitive information of staff and our customers.

To ensure all staff across the Council are aware of, and understand the importance of, data protection and confidentiality.

To assist the Council to comply with all requirements of the DPA.

To ensure procedures are in place across the Council for staff, contractors and members regarding disclosure of personal information.

To increase the awareness of data subjects to the amount of personal data processed and stored by the Council about them and advise them of their rights under the data protection legislation.

To ensure all staff receive appropriate data protection training, with regular updates or when significant data protection guidance changes.

3.0 POLICY SCOPE

This policy applies to

- all substantive and temporary employees of Mid Ulster District Council
- any individual including contractors, volunteers and others who work on behalf of the Council
- all work experience and other students
- Councillors

This policy outlines the behaviours and responsibilities expected in order to ensure the Council continues to fulfil its obligations under the Data Protection Act 2018 and their related and all subsequent Data Protection legislation.

It applies to all data that the Council holds relating to identifiable individuals,
This can include:

Personal information	**Special category personal data** Special category data is personal data, which GDPR considers sensitive and deserving of extra attention:
First name & family name or surname address telephone numbers date of birth age qualifications training records financial information licensing information enforcement action complaint information	racial or ethnic origin religious or other philosophical beliefs political opinions trade union membership physical or mental health or condition sexual orientation. offences (including alleged offences) processing of genetic data processing biometric data for the purposes of identifying a natural person health data

This list is intended as a guide and is not exhaustive.

4.0 LINKAGE TO CORPORATE PLAN

With reference to Mid Ulster District Council's Corporate Plan 2015-2019, this policy contributes toward the vision of professional and trustworthy services and contributes to the delivery of the Corporate Theme 'Delivering for our people' : 1.1 High performing services focused on customer need and value for money.

5.0 DATA PROTECTION PRINCIPLES

5.1 The legislation places a responsibility on every data controller(Council) to process any personal data in accordance with the eight principles. More detailed guidance on these principles can be found in the link to the ICO's website (www.ico.gov.uk).
In order to comply with its obligations, Mid Ulster District Council undertakes to adhere to the eight principles:

5.11) Process personal data fairly and lawfully.
Council will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

5.12) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.
Council will ensure that the reason for which it collected the data originally is the only reason for which it processes the data, unless the individual is informed of any additional processing before it takes place.

5.13) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.
Council will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms and mechanisms for collecting data will always be drafted with this mind.

5.14) Keep personal data accurate and, where necessary, up to date.
Council will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the Council if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Council to ensure that any notification regarding the change is noted and acted on.

5.15) Only keep personal data for as long as is necessary.
Council undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Council will regularly review of the information held and destroy it in accordance with its information and retention schedule. Council will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste).

5.16) Process personal data in accordance with the rights of the data subject under the legislation.
Individuals have various rights under the legislation including a right to:

- be told the nature of the information the Council holds and any parties to whom this may be disclosed.
- prevent processing likely to cause damage or distress.
- prevent processing for purposes of direct marketing.
- be informed about the mechanics of any automated decision taking process that will significantly affect them.
- not have significant decisions that will affect them taken solely by automated process.
- sue for compensation if they suffer damage by any contravention of the legislation.
- take action to rectify, block, erase or destroy inaccurate data.
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened.

Council will only process personal data in accordance with individuals' rights.

5.17) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.
Council will ensure that all personal data is accessible only to those who have a valid reason for using it.
Council will implement appropriate and reasonable security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):e.g.

- keeping all personal data in a lockable cabinet with key-controlled access.
- Maintaining information security processes, procedures, physical and technical controls and policies to protect all personal data held.
- Maintain systems to protect personal data from malicious attack affecting its confidentiality ,integrity and availability.
- Operate appropriate measures for the deletion of personal data on manual and electronic formats.

5.18) Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.2 Our legal basis for using personal data

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, even deleting it – will have an acceptable legal basis. There are six of these:

- Where it involves the exercise of a public function – i.e. most activities of most government, local government and other public bodies.
- Where it is *necessary* in connection with a contract between the Council and the individual.
- Where it is *necessary* because of a legal obligation.
- Where it is *necessary* in our legitimate interests, as long as these are not outweighed by the interests of the individual.
- Where it is *necessary* in an emergency, to protect an individual's 'vital interests'.
- Consent from the individual (or someone authorised to consent on their behalf).

Where we are basing our processing on consent we will be able to 'demonstrate' that we hold consent.

Council will ensure that any data collection is transparent and the individual will be aware of the purpose for same , e.g. in a short statement on a form(fair collection statement) explaining the use of that data etc.

5.3 Disclosure of Data

Only disclosures which have been notified under the Council's privacy notices and therefore staff should exercise caution when asked to disclose personal data held on another individual or third party.
Council undertakes not to disclose personal data to unauthorised third parties, but legitimate disclosures may occur e.g.:

- the individual has given their consent to the disclosure.
- the disclosure has been notified to the OIC and is in the legitimate interests of
- the Council.
- the disclosure is required for the performance of a contract.
- There are other instances when the legislation permits disclosure without the consent of the individual.
-

In no circumstances will Council sell any of its databases to a third party.

5.4 Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the Council. Any individual can exercise this right verbally or in writing to the Data Protection Officer(DPO). (see appendix 1).
Any such request to access personal data is called a Subject access request. Any member of staff receiving a SAR should forward this to the DPO.
Under the terms of the legislation, any such requests must be responded to within one month of receipt.

In most cases Council cannot charge a fee to comply with a subject access request but where the request is manifestly unfounded or excessive Council may charge a "reasonable fee" for the administrative costs of complying with the request.

The Council will ask for information necessary to confirm the identity of the requester.

Requested personal data will be retrieved from the relevant department and screened by the DPO before completion within a month of receipt. Failure to meet SAR timescales will expose the council to risk of fines and further action from the ICO.

5.5 Council Marketing

The Council may hold and process some personal data for marketing purposes, e.g.
Customer information for arts and cultural programmes and other events
Photographs for use in printed and online promotional activity.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted Council access only. Therefore, it is Council policy to offer an opportunity to opt-in for marketing purposes when collecting the information.

5.6 Email

It is the policy of Council to ensure that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Council's email.

Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice Regulations, any email sent to or from the Council may be accessed by someone other than the recipient for system management, security purposes and other reasons as set out in the email and instant messaging policy.

5.7 CCTV

There are some CCTV systems operating within Council and town centres for the purpose of protecting the Public and or Council property. Council has carried out privacy impact assessments in respect of these installations and will only process personal data obtained by the CCTV system in a manner which ensures compliance with our policy and applicable legislation.

5.8 Breach of Personal Data

Any incident or action that affects the confidentiality, integrity or availability of personal data could potentially be a breach that Council may have to report to the ICO within 72 hours of becoming aware of it. Such reports will be sent to the ICO using appendix 4 to the ICO in accordance with their latest guidelines.

In short, there will be a personal data breach whenever

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation.
- or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Notification Requirement: such incidents must be brought to any member of the team in accordance with procedures defined in appendix 2. Council must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.(See appendix 2 for further details).

6.0 ROLES AND RESPONSIBILITIES

6.1 The Chief Executive is ultimately responsible for our compliance with data protection legislation.

As a public authority as defined under the legislation the Council has appointed a Data Protection Officer (see appendix 1)
The DPO's minimum tasks are defined as:

- to inform and advise the controller, its employees, and any associated processors about their obligations to comply with the GDPR and other relevant data protection laws such as Part 3 of the Bill;
- to monitor compliance with data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

Senior Management Team
The Senior Management Team are responsible for all day-to-day data protection matters, and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the Council.

Compliance with the legislation is the personal responsibility of all members of the Council who process personal information. Potential breaches of this policy will be investigated and subject to Mid Ulster District Council's or other relevant disciplinary procedure.

Heads of Service and Managers

Managers within every service or business area are responsible for implementing and ensuring compliance with data protection procedures. This includes the requirement to take all reasonable steps to ensure compliance by third parties.

SMT &Managers must contact the DPO or Solicitor if they are unsure about any aspect of the DPA requirements including

- what security or other measures they need to implement to protect personal data.
- the lawful basis which they are relying on to process personal data
- consent matters for processing personal data
- privacy notices or other transparency information
- the retention periods.
- the transfer of personal data outside the European Economic Area (EEA)
- engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (by Design and by Default)
- to use personal data for purposes other than those for which it was originally collected
- activities involving automated processing.
- help with any contracts or other areas in relation to sharing personal data with third parties (including our contractors)
- sharing data with another organisation or person in a way which is new or could affect data subjects' rights.
- Any potential or suspected breach or incident relating to personal data.(see Appendix 2)

All Staff

Everyone working for us or on our behalf is required to comply with this policy.
Everyone working for us or on our behalf is responsible for ensuring that they understand and follow this policy and other procedures relating to the processing and use of personal data and support us in complying with data protection legislation.

Staff who handle personal data will be required to complete mandatory data protection training.

Elected Members
Members Elected members will endorse the policy, its implementation and procedures.

Compliance
We will regularly review monitor and audit the systems and processes under our control to ensure they comply with this policy. We will investigate any alleged breach of this policy in line with the breach process in Appendii 2&3 and assess whether the incident is reportable

to the ICO using Appendix 4. An investigation could result in us taking action up to and including dismissal; removal from office; or, termination of a contract for services.

7.0 IMPACT ASSESSMENTS

7.1 Equality Screening & Impact

7.2 The policy has been subjected to equality screening in accordance with the Council's screening process. The outcome of the screening has screened this policy out.

7.3 Rural Needs Impact

The policy has been subjected to a rural needs impact assessment and this policy has considered the assessment during the policy development.

7.4 Staff & Financial Resources

This policy requires resources to train those staff handling personal data. Online E Learning and class based learning may be used. The council will assign sufficient resources to accommodate these training requirements.
No issues have been identified which would significantly impact on the Councils resources and delivery of its business as a result of this policy being implemented.

8.0 SUPPORT AND ADVICE

8.1 Advice and guidance on the implementation of this should be sought from the DPO or Council solicitor.

9.0 COMMUNICATION

9.1 Council will ensure that all staff processing personal data receive required training on data protection.
Council will ensure that those who are responsible for implementing this policy, or responding to subject access requests under this policy, will receive additional training and resources to help them understand and to comply with them.

9.2 This policy will be published on the Intranet and brought to the attention of all staff within the Council.

10.0 MONITORING & REVIEW ARRANGEMENTS

10.1 Implementation of this policy will be monitored and a formal review undertaken 24 months from its effective date.

Appendix 1

Mid Ulster District Council

Data Controller Name: Mid Ulster District Council

Address: c/o Dungannon Office, Circular Road, Dungannon, BT71 6DT

Telephone: 03000 132 132

Data Protection Officer Name: Barry O'Hagan

Telephone: 03000 132 132

Email: barry.ohagan@midulstercouncil.org

Council's Data Protection Registration reference: **ZA086387**

Appendix 2

Data Breach Procedure and Response Plan (draft)

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation.
- or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Notification Requirement: when a security incident takes place, Council must quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

Alert Response

The data breach process is initiated when anyone notices that a suspected or alleged or actual data breach occurs. The DPO or any member of the Data Breach Response team must be notified as soon as possible and not later than 24hrs from becoming aware .

The data response team is made up of ;

The Data Protection Officer

Director of Finance

Any member of the IT team

Where a privacy data breach is known to have occurred (or is suspected) any member of response team staff who becomes aware of this must, within 24 hours, alert a member of data response team in the first instance.

The Information that should be provided (if known) at this point includes:

- When the breach occurred (time and date)
- Description of the breach (type of personal information involved)
- Cause of the breach (if known) otherwise how it was discovered
- Which system(s) if any are affected?
- Which directorate/faculty/institute is involved?
- Whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach)

A template can be found at **Appendix 3** to assist in documenting the required information.

Assess and determine the potential impact.

Once notified of the information above, the team must consider whether a privacy data breach has (or is likely to have) occurred and make a preliminary judgement as to its severity. The DPO should be contacted for advice.

Primary role of the Response Team

There is no single method of responding to a data breach and each incident must be dealt with on a case by case basis by assessing the circumstances and associated risks to inform the appropriate course of action.

The following steps may be undertaken by the Response Team (as appropriate):

•Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system.

•Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach having regard for the information outlined above.

•Call upon the expertise of, or consult with, relevant staff in the circumstances.

•Engage an independent cyber security or forensic expert as appropriate.

•Assess whether serious harm is likely

•Make a recommendation to the DPO whether this breach constitutes a Notifiable incident for the purpose of mandatory reporting to the ICO and the practicality of notifying affected individuals. Consider developing a communication or media strategy in conjunction with the marketing and communications team including the timing, content and method of any announcements to staff or the media.

The Response Team must undertake its assessment within 48 hours of being convened.

The DPO will provide periodic updates to the Chief Executive and or deputy as deemed appropriate.

Appendix 3

Data Incident Reporting Form

Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Technology (IT) security incident. All items completed should be based on information that is currently available. This form may be updated and modified if necessary.

1. Contact Information for this Incident	
Name:	
Title:	
Work Phone:	
Mobile Phone:	
Email address:	

2. Incident Description.

Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.

☐ Loss / Compromise of Data	☐ Other Organisations' Systems Affected
☐ Damage to Systems	☐ Damage to the Integrity or Delivery of Critical Goods, Services or Information
☐ System Downtime	☐ Violation of legislation / regulation
☐ Financial Loss	☐ Unknown at this time

Provide a brief description of the impact:

Provide a brief description of data that was compromised:

5. Who Else Has Been Notified?
Provide Person and Title:
6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

☐ No action taken ☐ System Disconnected from network ☐ Updated virus definitions & scanned system	☐ Restored backup from tape ☐ Log files examined (saved & secured) ☐ Other – please describe:
Provide a brief description:	
7. Incident Details	
Date and Time the Incident was discovered:	
Has the incident been resolved?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Please submit this completed form to :Head of IT

Barry.ohagan@midulstercouncil.org

Appendix 4

ICO Reportable incident form

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- ○ Initial report
- ○ Follow-up report

(Follow-up reports only) ICO case reference:

About the breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?

- ○ Yes
- ○ No
- ○ Don't know

How did you find out about the breach?

When did you discover the breach?

Date:

Time:

When did the breach happen?

Date:

Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data
- ☐ Basic personal identifiers, eg name, contact details
- ☐ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data
- ☐ Genetic or biometric data
- ☐ Criminal convictions, offences
- ☐ Not yet known
- ☐ Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

- ☐ Employees

- [ ] Users
- [ ] Subscribers
- [ ] Students
- [ ] Customers or prospective customers
- [ ] Patients
- [ ] Children
- [ ] Vulnerable adults
- [ ] Not yet known
- [ ] Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

- ○ Very likely
- ○ Likely
- ○ Neutral - neither likely nor unlikely
- ○ Unlikely
- ○ Very unlikely
- ○ Not yet known

Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

- ○ Yes
- ○ No
- ○ Don't know

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

- [ ] Confidentiality

☐ Integrity

☐ Availability

(Cyber incidents only) Impact on your organisation

○ High - you have lost the ability to provide all critical services to all users

○ Medium - you have lost the ability to provide a critical service to some

○ Low - there is no loss of efficiency, or a low loss of efficiency, and you can still provide all critical services to all users

○ Not yet known

(Cyber incidents only) Recovery time

○ Regular - you can predict your recovery time, with existing resources

○ Supplemented - you can predict your recovery time with additional

○ Extended - you cannot predict your recovery time, and need extra resources

○ Not recoverable - recovery from the incident is not possible, eg backups can't be restored

○ Complete - recovery is complete

○ Not yet known

Had the staff member involved in this breach received data protection training in the last two years?

○ Yes

○ No

○ Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature*

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, eg confirmed data sent in error has been destroyed, updated passwords, planning information security training.

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed*

Have you told data subjects about the breach?

- Yes, we've told affected data subjects
- We're about to, or are in the process of telling data subjects
- No, they're already aware
- No, but we're planning to
- No, we've decided not to
- We haven't decided yet if we will tell them or not
- Something else (please give details below)

Have you told, or are you planning to tell any other organisations about the breach?

eg the police, other regulators or supervisory authorities. In case we need to make contact with other agencies

- Yes
- No
- Don't know

If you answered yes, please specify

About you

Organisation (data controller) name

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name:

Email:

Phone:

Sending this form

Initial report

If this is your initial report, please send your completed form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report

If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.