Report of:	Meeting	Date
Corporate Director Resources (Section 151 Officer)	Audit Committee	26 November 2020

APPROVAL OF THE COUNCIL'S DATA PROTECTION POLICY AND PROCEDURES

1. Purpose of report

1.1 Approval of the council's Data Protection Policy and Procedures which includes the council's incident / breach reporting and investigation instruction.

2. Outcomes

2.1 The ability to demonstrate that the council has arrangements in place to ensure compliance with the General Data Protection Regulations (GDPR) and other data protection laws.

3. Recommendation

3.1 Members are asked to approve the attached Data Protection Policy and Procedures and incident / breach reporting and investigation instruction at Appendix 1.

4. Background

4.1 In March 2018 the Audit Committee were given delegated responsibility for ensuring the council is complaint with the GDPR and other data protection law, e.g. the Data Protection Act 2018. The Committee's Terms of Reference states; "To receive updates and reports from the Head of Governance (Data Protection Officer) and to approve policies in relation to compliance with the Data Protection Act and Regulations made under the Act".

4.2 Wyre Council takes its responsibilities with regards to the management of the requirements of the GDPR and other data protection requirements very seriously. This policy sets out how the council manages those responsibilities.

4.3 The council obtains, uses, stores and processes personal data relating to our residents / customers, potential, current and former staff, contractors and partners, collectively referred to in this policy as 'data subjects'.

When processing personal data, the council is obliged to fulfil individuals' reasonable expectations of privacy by complying with the GDPR and other relevant data protection legislation (The Data Protection Act 2018).

4.4 This policy and guidance seeks to ensure that the council;

- is clear about how personal data must be processed and the expectations for all those who process personal data on its behalf;
- complies with the data protection law and with any other good practice around data processing;
- protects its reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights; and
- protects itself from risks of personal data breaches and other breaches of data protection law.

5. Key Issues and proposals

5.1 The Data Protection Policy and Procedures and incident / breach reporting and investigation instruction was last reviewed and approved by the Audit Committee in November 2019 and is attached at Appendix 1. Following a review by the council's Data Protection Officer, only one minor change, relating to the council's approach to Data Protection Training (para 16.2) has been made.

Financial and legal implications	
Finance	There are no specific financial implications arising from the adoption of this policy.
Legal	The council's Data Protection Policy and Procedures assist the council in ensuring it meets the requirements of the General Data Protection Regulations and other data protection law.

Other risks / implications: checklist

If there are significant implications arising from this report on any issues marked with a ✓ below, the report author will have consulted with the appropriate specialist officers on those implications and addressed them in the body of the report. There are no significant implications arising directly from this report, for those issues marked with a x.

risks/implications	**✓ / x**
community safety	X
equality and diversity	X
sustainability	X
health and safety	X

risks/implications	**✓ / x**
asset management	X
climate change	X
ICT	✓
Data protection	✓

Processing Personal Data

In addition to considering data protection along with the other risks/ implications, the report author will need to decide if a 'privacy impact assessment (PIA)' is also required. If the decision(s) recommended in this report will result in the collection and processing of personal data for the first time (i.e. purchase of a new system, a new working arrangement with a third party) a PIA will need to have been completed and signed off by Data Protection Officer before the decision is taken in compliance with the Data Protection Act 2018.

report author	telephone no.	email	date
Joanne Billington	01253 887372	joanne.billington@wyre.gov.uk	18.11.2020

List of background papers:		
name of document	date	where available for inspection
None		

List of appendices

Appendix 1 – Data Protection Policy and Procedures

Data Protection Policy and Procedures

Version 2.0 – November 2020

1.0 Introduction

1.1 The processing of personal data is essential to many of the services and functions carried out by local authorities. Wyre Council ('the Council') recognises that compliance with data protection legislation (including the General Data Protection Regulations ('GDPR'), the Data Protection Act 2018 ('DPA') and related legislation) will ensure that such processing is carried out fairly, lawfully and transparently.

1.2 Data protection legislation, and Article 8 of the European Convention on Human Rights recognise that the processing of personal data needs to strike a balance between the need for an organisation utilising personal data to function effectively, efficiently and in the wider public interest, and respect for the rights and freedoms of the individual(s) ('data subject(s)') to whom the personal data relates. This policy sets out how the Council intends to safeguard those rights and freedoms.

1.3 The Information Commissioner's Office (ICO) is an independent authority which has legal powers to ensure organisations comply with the DPA and GDPR. For more information on the role of the ICO, please go to www.ico.org.uk.

2.0 Scope

2.1 This policy applies to the collection, use, sharing and other processing of all personal data held by the Council, in any format including paper, electronic, audio and visual. It applies to all council staff. 'Staff' for the purposes of this policy includes all council officers, volunteers and agency staff.

3.0 Legal context

3.1 Reference to the following legislation and guidance may be required when reading this policy.

- The Data Protection Act 2018
- The General Data Protection Regulations
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998

3.2 Reference to the following internal council documents may also be required when reading this Policy;

- The Council's Constitution
- Employee's Code of Conduct
- ICT Computer Use Policy
- Security Incident Policy

- Records Management Policy
- Password Policy and User Guidance

4.0 Personal data processed by the Council

4.1 The Council processes personal data for many reasons, including in relation to the services it provides and in its role as an employer. In most instances the Council will be the data controller (usually alone, but sometimes jointly) in respect of the personal data it processes (i.e. it will determine the purpose and means of the processing); on occasion it may act as a data processor on behalf of another data controller.

4.2 Whether acting as a data controller in its own right, or on another's behalf as data processor, the Council will maintain a record of its processing activities and make this available to the Office of the Information Commissioner ('ICO') upon request. Information concerning the processing of personal data in respect of which the Council is a data controller will be communicated by the Council to data subjects by means of appropriate privacy notices.

4.3 The Council has an overarching privacy notice and individual service privacy notices that can be found on the Council's website.

4.4 The Council is committed to ensuring compliance with data processing legislation and will;

- Respect the rights of each individual;
- Be open and honest about the personal data it holds;
- Provide training and support to those handling personal data in the course of their duties;
- Notify the ICO annually, that it processes data. (This is a statutory requirement and notification must be kept up to date with any changes to the use of personal data being updated within 28 days.) The Council has two registration numbers Z5682712 (General processing) and ZA319367 (elected Members); and
- Inform the ICO and in some instances the data subject of any data breaches.

5.0 Data protection principles

5.1 The Council will comply with the principles relating to the processing of personal data set out in the GDPR by putting in place processes to ensure that personal data is:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (further processing for archiving purposes in the public interest, scientific or historical

research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject); and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 The Council shall be responsible for, and be able to demonstrate compliance with all the above principles.

5.3 Where the Council processes personal data as a 'competent authority' for 'law enforcement purposes' (i.e under statutory law enforcement functions) it shall do so in accordance with the version of the data protection principles set out in the Law Enforcement provisions of the DPA. Those principles are similar (but not identical) to the principles applying to more general processing of personal data detailed above.

5.4 'Law enforcement purposes' include the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public safety.

6.0 Legal basis for processing

6.1 The Council will ensure that it's processing of personal data (other than law enforcement processing) fulfils the appropriate general condition(s) for processing outlined in the GDPR. Where a 'special category' of personal data is processed (this includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purposes of identifying an individual, physical or mental health, sex life or sexual orientation), the Council will ensure that one of the additional conditions set out in relation to special category personal data in the GDPR is also met, along with any further requirements regarding the processing of sensitive personal data set out in other data protection legislation.

6.2 While not formally defined as a 'special category' of personal data under the GDPR, similar additional conditions and requirements also apply to personal data relating to criminal convictions and offences (including personal data relating to the alleged commission of offences and proceedings relating to the commission or alleged commission of offences). When processing such data the Council will ensure that the relevant additional conditions and requirements are met.

6.3 Where the Council processes personal data as a 'competent authority' for 'law enforcement purposes' it shall do so in accordance with the requirements of the law enforcement provisions of the DPA. In all cases such processing will only be carried out where the individual concerned has given their consent to the processing of their personal data for law enforcement purposes or where the processing is necessary for the performance of a task carried out for law enforcement purposes by a competent authority. Where such processing involves 'sensitive processing' (this is equivalent to the processing of special category personal data under the GDPR) the Council will ensure that the processing is strictly necessary and (unless the individual has consented to the processing) that one of the conditions for sensitive processing set out in the DPA is met.

7.0 Individuals' rights

7.1 Data protection legislation provides individuals with various rights. An individual's rights include:

- The right to be provided with specified information about the Council's processing of their personal data **('the right to be informed').**
- The right to access their personal data and certain supplementary information **('the right of access').**
- The right to have their personal data rectified, if it is inaccurate or incomplete **('the right of rectification').**
- The right to have, in certain circumstances, their personal data deleted or removed **('the right of erasure', sometimes knowns as 'the right to be forgotten').**
- The right, in certain circumstances, to restrict the processing of their personal data **('the right to restrict processing').**
- The right, in certain circumstances, to move personal data the individual has provided to the Council to another organisation **('the right of data portability').**
- The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the Council to stop processing that data **('the right to object').**

- The right, in relevant circumstances, to not be subject to decision-making based solely on automated processing **('Rights related to automated decision making, including profiling').**

7.2 In relation to the first right referred to above ('the right to be informed') in general the Council will:

- where the personal data is collected from an individual, provide them with specified privacy notice information, at the time the personal data is collected, for example when a member of public is signing up to receive a council service;

- where the personal data has not been obtained from an individual, provide them with specified privacy notice information within one month; if the Council uses personal data that it has not collected directly from an individual to communicate with that individual, it will provide the specified privacy notice information, at the latest, when the first communication takes place; if disclosure to another recipient of personal data that has not been collected directly from the individual is envisaged the Council will provide the specified privacy notice information, at the latest, before the data is disclosed.

7.3 It should be noted that there are limited specified circumstances in which the right to be informed will not apply. For further information go to www.ICO.org.uk

7.4 Where an individual exercises one of the other rights listed above, the Council will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:

- Where further time is necessary, taking into account the complexity and the number of the request(s) from the data subject, the period for responding will be extended by up to two further calendar months. Where such an extension is required the Council will notify the data subject that this is the case within one calendar month of receiving their request.

- Where the request(s) from a data subject are manifestly unfounded or excessive (in particular because of their repetitive character) the Council will ordinarily refuse the request(s). In exceptional cases the Council may instead exercise its alternative right in such circumstances to charge a reasonable fee that takes into account the administrative cost of complying with the request.

7.5 The Council recognises the fundamental nature of the individual rights provided by data protection legislation. The Council will ensure that all valid requests from individuals to exercise those rights are dealt with as quickly as possible and by no later than the timescales allowed in the legislation.

7.6 To minimise delays, and to help ensure that the Council properly understands the request being made, it is preferable for requests from data subjects wishing to exercise their data subject rights to be either in writing or made via the Council's on-line process. However, a valid request may also be made verbally.

7.7 The Council's dedicated email address for exercising individual rights is informationgovernance@wyre.gov.uk or individuals can use the council's online form available from the Council's website at;

https://www.wyre.gov.uk/info/200373/your_data_and_us

7.8 All requests from data subjects to exercise their data subject rights must:

- Be accompanied by, where necessary, proof of the identity of the data subject and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or authorised agent);

- Specify clearly and simply how the data subject wishes to exercise their rights – this does not mean that an individual needs to refer specifically to a particular right by name or legislative provision (for example, "I would like a copy of my employee file" is sufficiently clear to indicate that the right of access is being engaged);

- Give adequate information to enable the Council to determine whether the right is engaged and to comply (subject to any exemption(s)) if it is;

- Make it clear where the response should be sent; and

- Where relevant specify the preferred format in which any information disclosed to the data subject should be provided.

7.9 Data protection law allows exemptions from complying with data subject rights in specific and limited circumstances. The Council will normally apply the exemptions where they are engaged, unless it is satisfied that it is appropriate or reasonable not to do so.

7.10 If a data subject exercising one or more of their data subject rights is dissatisfied with the response received from the Council, they may ask for the matter to be dealt with by the Council's Data Protection Officer (DPO). Alternatively, a data subject also has the right to complain to the ICO if they believe that there has been an infringement by the Council of data protection legislation in relation to the data subject's personal data. A data subject may also pursue a legal remedy via the courts. Further information on the rights of data subjects is available from the ICO's website www.ico.org.uk.

7.11 Additional guidance for staff on how to deal with requests to exercise data subject rights is available via the Council's intranet.

8.0 Individuals' Rights – Law Enforcement Processing

8.1 The rules relating to an individual's rights are different where the Council processes personal data as a 'competent authority' for 'law enforcement purposes'. In those circumstances individuals have the following rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restriction of processing; and
- the right not to be subject to automated processing.

8.2 There are no equivalents to the right to object or the right to data portability. Also, the right of access, the right to rectification and the right to erasure or restriction of processing will not apply to 'relevant personal data' in the course of a criminal investigation or criminal proceedings.

8.3 'Relevant personal data' means personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority. Where an individual exercises their rights in respect of personal data that the Council is processing for law enforcement purposes the Council will ordinarily respond without undue delay and in any event within one calendar month. There is not an option for the Council to extend this for a further period in the case of complex or numerous requests, although the Council can refuse (or make an administrative charge for) manifestly unfounded or excessive requests.

9.0 Further legal requirements

9.1 The Council may be required to disclose personal data to a person or organisation other than the data subject by virtue of a court order, or to comply with other legal requirements, including those relating to the prevention or detection of crime, the apprehension/prosecution of an offender, or the collection of taxation/duties.

9.2 The Council may also, in appropriate circumstances, make discretionary disclosures of personal data to a person or organisation other than the data subject where it is permitted to do so by law. When deciding whether to exercise its discretion to disclose personal data in such circumstances the Council will always give proper consideration to the data subject's interests and their right to privacy.

9.3 External agencies, companies or individuals undertaking processing of personal data on behalf of the Council ("data processors") must be required to demonstrate, via a written contractual agreement, that personal data belonging to the Council will be handled in compliance with data protection legislation and that appropriate technical and organisational security measures are in place to ensure this. Any contractual agreement between the Council and a data processor will contain all the relevant elements specified in data protection legislation.

9.4 The Council will follow relevant guidance issued by the Government, the ICO and the Surveillance Camera Commissioner for users of CCTV and similar

surveillance equipment monitoring spaces to which the public, residents, service users and staff have access and will also strive to ensure that partner organisations involved in joint or multi-agency initiatives seek to do the same.

9.5 The Council reserves the right to monitor telephone calls, e-mail and internet access in compliance with relevant legislation. This will be handled in line with guidance issued by the ICO and the Investigatory Powers Commissioner's Office (IPCO).

10.0 Privacy by design and by default (Privacy Impact Assessments)

10.1 The Council's approach to compliance with data protection legislation will be underpinned by the principles of privacy by design and privacy by default. 'Privacy by design' means that the Council will take into account privacy issues from the very outset of planning for an activity that might involve the processing of personal data.

10.2 'Privacy by default' means that the Council will ensure that only personal data that is necessary for a specific purpose is processed. The Council will not collect more personal data than is needed for the purposes concerned, process it more than is necessary or store it longer than is needed.

10.3 When undertaking a new activity, privacy considerations will be embedded throughout. A Privacy Impact Assessment will need to be completed and signed off by the Council's DPO before the activity commences.

11.0 Records Management

11.1 The Council must manage and dispose of its records in accordance with the Council's Records Management Policy and service specific Information Asset Registers. It is essential that records are stored securely and the location of information is up to date at all times to enable the Council to process any requests for information (FOI's and SAR's) within the required timescales.

12.0 Information Security

12.1 Effective methods of security must be in place to help prevent the inappropriate disclosure or loss of personal data. The Council will process personal data in accordance with the DPA and GDPR and any other related Council policy and procedure to ensure appropriate physical, technical and organisational measures are in place.

12.2 Access to areas where data is stored and used must be controlled as follows;

- Paper files must be locked away when not in use and electronic systems must be password protected, with only authorised users being given access;
- Staff working away from the office must ensure records are adequately protected at all times, preventing damage, theft / loss and unauthorised access to personal data;
- Electronic data must be stored on the Council's servers and should be backed up each night to prevent the loss of valuable data;

- Personal data must not be stored on unencrypted portable equipment, e.g. laptops, mobile phones, tablet devices or memory sticks / pen drives. Staff are advised to contact ICT for assistance if they are wanting to transfer personal data out of the organisation;
- Desktop computers, laptops and tablet devices must be password protected and locked when left unattended during the day. Staff are required to log off and shut down all systems at the end of the working day;
- Staff must not disclose passwords to colleagues or use passwords belonging to other staff members.
- Confidential waste bins are located throughout the building and must be used for the destruction of personal data. The Council employs a contractor to shred all paper waste on site once a week, therefore, there is no requirement to shred any personal data prior to using the confidential waste bins.

13.0 Information Sharing

13.1 When personal data is collected, the data subject must be informed, via a privacy notice, what data the Council expects to share, with whom it is likely to be shared and in what circumstances. See 7.2 for guidance on when the data subject needs to be informed.

13.2 Non-sensitive personal data may be shared across Council departments and with contractors working on the Council's behalf for legitimate purposes, such as:

- Updating Council records;
- Providing services; and
- Preventing and detecting fraud.

13.3 Sensitive personal data is normally only disclosed with the informed consent of the data subject. However, there are circumstances in which personal data may be disclosed without obtaining the data subject's consent such as when safeguarding the data subject or others, and to assist with the prevention and detection of crime. For further guidance, refer to the ICO's website or speak to the Council's DPO.

13.4 Information sharing protocols / agreements should be in place between all Council and third parties when personal data is being shared. All agreements must be signed off by the DPO at which point a record of the data shared will be documented in the relevant information asset register.

13.5 Any sharing of Council-controlled personal data with other data controllers must comply with all statutory requirements and corporate policies. Where appropriate the Council will enter into a data sharing agreement before sharing personal data with another data controller, particularly where personal data is to be shared on a large scale and/or regularly. Any data sharing agreements must be signed off by the DPO and the Council's Legal Services Manager.

14.0 Secure Transfer of Data

14.1 The transfer of data in all formats (written, fax, email, phone or face to face) must be completed in a secure manner, ensuring the identity of the recipient has been verified. This will help prevent personal data being misplaced or disclosed in error.

14.2 Secure Email
When providing information by email, client details must not be placed in the subject heading. Be aware that when the recipient replies and includes your original email, the return email is not secure. Recipients should be made aware of this and be advised to refer to their own organisation's procedures. All emails that contain personal data must be encrypted. Password protecting the email or file is not sufficient protection to secure the contents. Employees should contact ICT if they do not know how to encrypt an email or a document that contains personal data.

14.3 Postal Mail
The Council has a data classification scheme in place that sets out how internal and external mail should be sent depending on its content.

14.4 Fax
When sending personal data by fax, it is imperative that the sender phones ahead to the receiver to ensure they are standing by the machine to receive the fax. The receiver must then confirm that the fax has been received in full.

15.0 Roles and Responsibilities

15.1 Everyone representing the Council has a duty to protect the information it holds, and access to personal data must be on a strict need to know basis. Personal data must not be disclosed without appropriate authorisation.

15.2 The Council has an Information Governance Group which is accountable for ensuring compliance with this policy across the Council. The work of the group will be supported by the Corporate Management Team and the Audit Committee who have delegated responsibility for ensuring the Council's compliance to the DPA and GDPR. The group's membership consists of the DPO, the Information Governance Manager (Deputy DPO), Head of ICT and the Legal Services Manager.

15.3 The Council will ensure that:

- The DPO reports to the highest management level of the Council in respect of their duties as DPO, in this instance, this is the Corporate Management Team.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Individuals handling personal data will be trained to an appropriate level in the use and control of personal data.
- All staff handling personal data know when and how to report any actual or suspected data breach, and that appropriately trained staff manage any breach correctly, lawfully and in a timely manner.

- Breaches will be reported to the ICO where such reporting is mandatory or otherwise appropriate and shall be done within the required timescales.
- It monitors and reviews its processing activities to ensure these are compliant with data protection legislation.
- Where there is any new or altered processing of personal data it will take appropriate steps (including where necessary a privacy impact assessment) to identify and assess the impact on data subjects' privacy as a result of the processing of their personal data.
- Appropriate privacy notices are maintained to inform data subjects of how their data will be used and to provide other mandatory or relevant information; and
- This policy remains consistent with the law, and any compliance advice and codes of practice issued from time to time by the ICO is incorporated.

15.4 Elected Members may have access to, and process personal data in the same way as employees and therefore must comply with the six data protection principles. These can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/

15.5 As data held on Council systems may be used by Elected Members in their roles, the data controller may be the Elected Member or the Council individually, jointly or on behalf of the other. Notification must be arranged as follows:

- When acting on behalf of the Council, Elected Members can rely on the Council's legal basis and notifications for processing,
- When acting on their own behalf, for example, when dealing with complaints made by local residents, Elected Members are data controllers in their own right, therefore must themselves ensure they comply with the DPA and the GDPR; and
- When campaigning within their own political party (unless Independent Members), Members may rely on the legal basis and notification for processing of their own party.

15.6 From the 1 April 2019, the requirement for Elected Members to pay a registration fee to the ICO was abolished. Elected Members are now exempt from paying a fee, unless they process personal data for purposes other than the exercise of their functions as an Elected Member. For example, if they have their own business or they are using CCTV for business or crime prevention purposes in connection with that business, then a fee will still apply.

15.7 Whilst the majority of the Council's Elected Members will be exempt from paying a fee and having to register with the ICO, they are still Data Controllers in their own right and therefore have data protection responsibilities. This

means they are responsible for making sure all personal data handled complies with the requirements of the DPA and GDPR. All Elected Members have been issued with guidance on how they can achieve this. They have also been provided with a privacy notice which they can distribute to their constituents.

15.8 Elected Members must attend all training recommended to them and take the necessary steps to ensure the Council's data is stored safely in accordance with any Council policy and procedure. They must store all Council data separately from data relating to their ward and political party work.

16.0 Training

16.1 The Council recognises that data protection training is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with data protection legislation could lead to serious consequences, and in some cases may result in significant fines or criminal prosecution.

16.2 All data protection training provided by the Council is mandatory and Line Managers are responsible for ensuring that all staff attend and that staff are given the necessary time to attend. The Council provides all new starters with an induction pack which includes the Data Protection Policy and Procedures and Incident / Breach Reporting and Investigation Instruction. All staff are asked to sign to confirm they have read and that they understand the content of both documents. Whilst previously the Council used an e-learning video and tests to train all its staff on data protection and information security, access to this software is no longer permitted. At the time of this policy review, the Council was in the process of looking for a corporate e-learning training platform what would include both Data Protection and Information Security training modules.

16.3 Some post-holders are required to undertake further information governance or data protection training where appropriate for a particular role or within a specific service area, for example the DPO and their deputy and staff with specific responsibility for processing Freedom of Information (FOI's) Act requests and Subject Access Requests (SAR's).

17.0 Reporting a potential data breach

17.1 In the event of a suspected data breach it is essential that staff follow the guidance for reporting potential breaches (attached at Appendix A). Adhering to this guidance will ensure that all risks are identified and mitigated, the appropriate people and organisations are informed, and communication is prepared to help prevent damage to the data subject and the Council's reputation.

17.2 All incidents, including near misses, should be reported to the DPO or the Deputy DPO. Failure to report an incident could result in disciplinary action including dismissal (see 19.1).

17.3 All incidents are logged into a 'data incident log' which is maintained by the DPO and monitored by the Information Governance Group. It is also available for inspection by the ICO.

17.4 It should be noted that at present, the council has a separate 'Security Incident Protocol' for the reporting and recording of any ICT related incidents, e.g. loss of equipment, viruses, bogus emails etc. However, this protocol does not supersede the guidance attached at Appendix A.

18.0 Governance and Distribution

18.1 The ownership of this policy sits with the Information Governance Group. The group will review the policy annually with any changes being submitted to the Audit Committee for approval.

18.2 The policy will be displayed on the Council's intranet and also the Council's website on the data protection web page:

https://www.wyre.gov.uk/info/200373/your_data_and_us

19.0 Disciplinary action and criminal offences

19.1 Serious breaches by staff of this policy caused by deliberate, negligent or reckless behaviour could result in disciplinary action including dismissal and may even give rise to criminal offences.

20.0 Sources of information and guidance

20.1 This policy is supported by training, awareness and additional guidance made available to staff on the Council's intranet. The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of information law for use by organisations and the public. Please see www.ico.org.uk

20.2 Other useful contact details

Data Protection Officer	01253 887372
Deputy Data Protection Officer	01253 887503
Legal Services Manager	01253 887214
Information Commission Officer helpline	0303 123 1113
ICT helpdesk	01253 887652 / 887425

Appendix A

Incident / breach reporting and investigation instruction

1.0 Introduction

1.1 Wyre Council is obliged under Data Protection law to investigate any breaches of security that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data when it is being used in any content or location.

1.2 The organisation needs to take steps as quickly as possible to recover any data involved in the incident or otherwise contain the spread or effects of the incident, whilst trying to ensure that the cause of the incident is properly identified. At Wyre Council, this responsibility falls to the Data Protection Officer (DPO) or the Deputy DPO.

1.3 Once an incident comes to light, a decision must be made by the DPO or their Deputy within 72 hours about whether to inform the Information Commissioner, and subsequently, whether to inform the affected individuals.

1.4 A genuine accident, mistake or theft that could not have been prevented is not considered to be a breach of Data Protection law, whereas a failure to implement proper security measures, whether technical or practical, to protect data is almost certainly a breach. Either way, they both need to be reported to the DPO or their Deputy and investigated thoroughly.

2.0 What to look out for and what should I report?

2.1 Losses and theft

- Loss or theft or paper documents / equipment containing council / personal data, especially sensitive or confidential information;
- Unauthorised access to, tampering with or use of ICT systems or equipment;
- Unauthorised changes to system hardware, firmware or software; or
- A deliberate attempt by a third party to steal data.

2.2 Mishandling

- Emails, post, faxes or other correspondence sent to the wrong person or destination, especially where the data is sensitive or the incidents are repeated;
- Wrong data or files attached to correspondence when sent out;
- Data or equipment on which data is stored is not securely disposed of; or
- Data or equipment is left in vacated buildings or furniture containing records is disposed of without records being cleared out.

2.3 Improper and inappropriate use

- Improper use of ICT system;
- Use of non-work email, equipment or storage for work purposes; or

- Failure to revoke access from leavers, contractors or people changing job roles.

2.4 Electronic and operational

- Malware attacks (viruses, ransomware, worms, Trojan horses);
- Unauthorised disruption of service, phishing attacks etc, or;
- System failure, crashes, environmental failures and operator errors. These may have security implications and should be treated as incidents.

3.0 How should I report one of the above?

3.1 Any suspected data breaches must be reported immediately in the first instance to the DPO or Deputy DPO. In the instance that neither officer is available, your Director or Service Manager should be informed. Contact details for the DPO and the Deputy DPO are as follows;

Data Protection Officer	Joanne Billington	01253 887372
Deputy Data Protection Officer	Joanne Porter	01253 887503

Alternatively, you can email the Council's dedicated incident reporting mailbox informationgovernance@wyre.gov.uk

3.2 Given that the organisation has a responsibility to notify the ICO where applicable within 72 hours of the identification of a breach, it is imperative that officers report incidents immediately, to allow the 72 hour timescale to be adhered to.

3.3 All documentation in relation to the incident must be collated and held securely until further instruction is given by the DPO or Deputy DPO. The DPO or Deputy will ask you for a 'written statement of fact'. Which is basically a detailed account of how the incident occurred, what data has been lost or put at risk and any other information that is important to the investigation.

3.4 It should be noted at this stage, any investigation is carried out in an informal manner with the primary objective being to ascertain if an 'actual breach' has occurred and if the breach has or could cause harm or damage to an individual or the organisation.

3.5 Staff under no circumstances should alert the data subject, the ICO or any third party to the suspected incident. The decision to notify the individuals concerned, the ICO and any third parties is the responsibility of the DPO or the Deputy DPO following a full investigation.

3.6 Failure to report an incident or adhere to paragraphs 3.1 – 3.5 above could lead to disciplinarily action.

4.0 Management of a data breach / incident

4.1 Once it has been identified that an actual data breach has occurred, it is important that the Council has an effective, documented plan of how they will deal with the incident. The DPO or the Deputy DPO is responsible for

ensuring that all reported incidents are dealt with as quickly as possible, in a transparent and consistent way.

4.2 The ICO recommends that as part of the investigation, the DPO or Deputy DPO will take the following four steps;

- Containment and Recovery
- Assessment of Risks
- Notification
- Evaluation and Response

4.3 The DPO or Deputy DPO may ask for your involvement at any stage of the investigation and it is expected that full participation and cooperation will be given. Where it is deemed that deliberate obstruction or withholding of information is taking place, this may lead to the council taking disciplinary action.

4.4 For further information on the four steps detailed at 4.2, please refer to the Data Protection page on the Council's intranet 'carrying out an investigation'.

https://wyregovuk.sharepoint.com/sites/Governance/SitePages/Data-protection.aspx