HUMBERSIDE FIRE AND RESCUE SERVICE

Service Improvement

Data Protection Policy

Owner	**Executive Director of Corporate Services**
Responsible person	**Head of Corporate Assurance**
Date Written	**May 2018**
Date of last review	**August 2024**
Date of next review	**August 2025**
EIA Reviewed	**August 2024**

What we must do well

How we support our communities

We value and support the people we employ

We efficiently manage the Service

CONTENTS

1. INTRODUCTION

The purpose of data protection legislation[1] is to protect the 'rights and freedoms' of natural persons (i.e. living individuals).

Data protection legislation applies to all data controllers that are established in the UK, who process the personal data of data subjects. It also applies to data controllers outside of the UK that process personal data in order to offer goods and services or monitor the behaviour of data subjects who are resident in the UK.

The Information Commissioner's Office (ICO) oversees compliance and promotes good practice, regulating all organisations and individuals who process personal data.

This Data Protection Policy applies to all personal data held by the Humberside Fire & Rescue Service (HFRS). The policy aims to ensure those individuals' rights and freedoms are protected, preventing personal data being mistreated or used to deny access to services. The policy will be used to ensure that the personal data the Service holds is used fairly and lawfully, in line with data protection legislation.

In order to operate effectively, the Service has to process personal information about people with whom it works. These may include members of the public, parents/guardians, current, past and prospective employees and suppliers. In addition, it is required by law to process information in order to comply with the requirements of central government.

The Service is committed to ensuring compliance with data protection legislation. The Service regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between the Service and those with whom it carries out business. The Service fully endorses the principles of data protection by design and default. To this end, the Service will ensure its Data Protection Officer is able to fulfil their tasks as defined in data protection legislation.

Third parties who have access to personal data will be expected to have read and understood this policy. No third party will be able to access personal data without being committed to having obligations no less onerous than the Service. The Service will make every effort to ensure data subjects can exercise their rights. Any breach of data protection legislation will be dealt with as a matter of urgency. If required, breaches will be reported to the appropriate authorities and where necessary, dealt with as a criminal offence. The Service is committed to working with the ICO in all areas relating to personal data.

This policy will be reviewed on an annual basis to ensure that it reflects changes to existing legislation and incorporates any new legislation.

[1] "The data protection legislation" means—
(i) the UK General Data Protection Regulation (UK GDPR) (ii) the Data Protection Act 2018 (DPA 2018) to the extent that it relates to processing of personal data and privacy; (iii) all applicable Law about the processing of personal data and privacy.

Core Code of Ethics

HFRS has adopted the Core Code of Ethics for Fire and Rescue Services. The Service is committed to the ethical principles of the Code and strives to apply them in all we do, therefore, those principles are reflected in this Policy.

National Guidance

Any National Guidance which has been adopted by HFRS, will be reflected in this Policy.

2. EQUALITY, DIVERSITY AND INCLUSION

HFRS has a legal responsibility under the Equality Act 2010, and a commitment, to ensure it does not discriminate either directly or indirectly in any of its functions and services or in its treatment of staff, in relation to race, sex, disability, sexual orientation, age, pregnancy and maternity, religion and belief, gender reassignment or marriage and civil partnership. It also has a duty to make reasonable adjustments for disabled applicants, employees and service users.

3. AIM and OBJECTIVES

To ensure that the Service has the structures and procedures in place to protect the rights and freedoms of individuals.

That both the Service and its employees are aware of their responsibilities with regard to data protection legislation.

That the Service operate in compliance with data protection legislation.

4. ASSOCIATED DOCUMENTS

- Equality Impact Assessment
- Legal References
  - Data Protection Act 2018
  - General Data Protection Regulation (Regulation (EU) 2016/679) as retained in UK domestic law)
  - Law Enforcement Directive (Directive (EU) 2016/680)
  - Human Rights Act 1998
  - Freedom of Information Act 2000
  - Privacy and Electronic Communications (EC Directive) Regulations 2003
  - Age-appropriate design: a code of practice for online services
  - Information Commissioner's Office (ICO)

- National Guidance
  There is no specific national guidance relevant to this policy.

- Information Security Policy
- Information Classification Policy
- Internet, E-Mail and Instant Messaging Policy
- Privacy and Consent Policy Delivery Guidance
- Data Protection Impact Assessment Policy Delivery Guidance
- Data Protection Request (inc SAR) Policy Delivery Guidance
- Records Management and Data Quality Policy
- Disposal and Destruction of Records Policy Delivery Guidance
- Personal Data Breach Notification Policy Delivery Guidance
- Safeguarding Policy
- Disclosure and Barring Service Policy
- Surveillance Camera Policy
- Disciplinary Policy
- Core Skills Framework
- Data Protection – Guide for Employees
- Data Protection – Guide for Managers

5. DEFINITIONS

For the purposes of this policy, the following definitions are in relation to Data Protection.

Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or, to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Category Data: Personal data revealing or concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Subject: Any living individual who is the subject of personal data held by an organisation.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling: Is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal Data Breach (PDB): A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

There is an obligation on data controllers to consider informing the ICO of a reported personal data breach. However, where any breach is likely to adversely affect the personal data or privacy of the data subject, the ICO must be notified

Information Society Services: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

Consent: In relation to the processing of an individual's personal data means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.

Third Party: A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

6. RESPONSIBILITIES AND ROLES OF THE SERVICE

The Service is a data controller as defined by data protection legislation. It is the responsibility of the Strategic Leadership Team to ensure compliance with data protection legislation. However, the Corporate Assurance Section is responsible for ensuring compliance within the day-to-day activities of the Service.

All those in managerial or supervisory roles throughout the Service are responsible for encouraging good information handling practices. Compliance with data protection legislation and this policy is the responsibility of all employees.

Employees are responsible for ensuring that any personal data about them and supplied by them is accurate and up to date. All employees who process personal data are responsible for their own compliance with data protection legislation and this policy. Failure to do so may result in the instigation of disciplinary procedures. The Service's Core Skills Framework sets out the specific training and awareness raising requirements.

The Service appointed Data Protection Officer (DPO) is accountable to the Corporate Assurance Section and the Strategic Leadership Team. The DPO's role is to provide advice to the Service and monitor compliance with data protection legislation.

The first point of contact for data protection matters is dataprotection@humbersidefire.gov.uk however, everyone has the right to speak to the DPO about their tasks.

7. POLICY DEVELOPMENT INCLUDING CONSULTATION

The following people and groups were consulted in development of this policy:

- HFRS Strategic Leadership Team
- HFRS Heads of Function
- Representative Bodies
- Data Protection Officer
- East Riding of Yorkshire Council *(as part of a Service Level Agreement)*

8. DATA PROTECTION PRINCIPLES

All processing of personal data must be conducted in accordance with data protection principles. The Service's policies and guidance are designed to ensure compliance with these principles.

Personal Data must be Processed Lawfully, Fairly and Transparently:

Lawful: a lawful basis must be identified before you can process personal data. These are often referred to as the "conditions for processing" and are listed in data protection legislation.

Fairly: in order for processing to be fair, the data controller has to make certain the personal data is only used in ways people would reasonably expect and not in a way that may adversely affect individuals. This applies whether the personal data was obtained directly from the data subjects or from other sources. The way in which the data is obtained must be open and honest.

Transparently: data protection legislation includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. The Service's Privacy and Consent Policy Delivery Guidance details how notices should be used across the Service, including the specific information that must be provided to the data subject.

Personal Data can only be collected for specific, Explicit and Legitimate Purposes (purpose limitation):

Data obtained for specified purposes must not be used for a purpose that differs from the reason it was collected, those formally notified to the ICO, outlined on the Service's records of processing activity or, in line with this Policy.

Personal Data must be adequate, relevant and limited to what is necessary for processing (data minimisation):

The Service must not collect information that is not strictly necessary for the purpose for which it is obtained. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or, link to a privacy statement and approved by the DPO. The DPO will ensure that, on a regular basis, all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive. The Service has a Data Protection Impact Assessment Policy Delivery Guidance to help meet this requirement.

Personal Data must be accurate and kept up to date with every effort to erase or rectify without delay (accuracy):

Data that is stored by the Service must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is the responsibility of the data subject to ensure that data held by the Service is accurate and up to date. Employees and suppliers are required to notify the Service of any changes in circumstance to enable personal records to be updated accordingly. Processes are in place to allow for the updating of records. It is the responsibility of the Service to ensure that any notification regarding change of circumstances is acted upon and recorded.

The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date. On a regular basis the DPO will review these processes and the retention dates for all personal data processed by the Service. Any data that is no longer required will be securely deleted/destroyed in line with the Disposal and Destruction of Records Policy Delivery Guidance.

Corporate Assurance is responsible for managing requests for erasure, rectification and objection from data subjects, in line with the Data Protection Request (inc SAR) Policy Delivery Guidance. Where personal data has been amended and that data is subject to a sharing agreement, Corporate Assurance will ensure the revised data is made available to the relevant third-party organisations, ensuring out of date or incomplete data is not used to inform decisions about the individuals concerned.

Personal Data must be kept in a form such that the data subject can be identified only as long as is necessary for processing (storage limitation):

Where possible, personal data will be minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Record Management and Data Quality Policy and, once its retention date is passed, it must be securely disposed of or destroyed in accordance with the Disposal and Destruction of Records Policy Delivery Guidance. Any data retention that exceeds the retention period must be approved by the Corporate Assurance Section. They must ensure that the justification is clearly identified and in line with the requirements of data protection legislation.

Personal data must be processed in a manner that ensures the appropriate security (integrity and confidentiality):

The Corporate Assurance Section will carry out risk assessments taking into account state of the art technical measures, the costs of implementation and the risk/likelihood to individuals if a security breach occurs, the effect of any security breach on the Service itself, and any likely reputational damage including the possible loss of customer trust.

Both HFRS (as controller) and its processors shall implement appropriate technical and organisational measures to ensure a level of security relevant to the risk, including where appropriate:

- the pseudonymisation and encryption of personal data.
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The policies and guidance identified in Section 4 (Associated Documents) above must also be considered.

The controller must be able to demonstrate compliance with the UK GDPR other principles (accountability):

Data protection legislation includes provisions that promote accountability and governance. These complement the transparency requirements. This additional accountability principle requires the Service to demonstrate that it complies with the principles and states explicitly that this is the Service's responsibility.

The Service demonstrates this compliance through this policy, its appropriate policy document, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, and establishing formal procedures in relation to data protection.

9. DATA SUBJECTS' RIGHTS

Data subjects have the following rights regarding data processing, and the data that is recorded about them.

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of any automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO assess whether any provision of the data protection legislation has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller (ported).
- To object to any automated profiling that is occurring without consent.

The Service makes every effort to ensure that data subjects may exercise these rights. A data subject may make a request as described in the Data Protection Request (inc SAR) Policy Delivery Guidance. These requests are, under normal circumstances, free of charge and will be dealt with in one month (although this timescale can be extended by two months in some circumstances).

Personal data must not be disclosed about a third party except in accordance with data protection legislation. If it appears absolutely necessary to disclose information about a third party, advice should be sought from the DPO.

Data subjects also have the right to complain to the Service in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled. This will be done in line with the Service's Complaints Policy.

10. DISCLOSURE OF DATA

The Service ensures that personal data is not disclosed to unauthorised third parties which includes family members, friends, suppliers, government bodies and other public sector organisations. All employees should exercise caution when asked by a third party, to disclose any personal data we hold on another individual.

All requests to provide data must be supported by the appropriate documentation. Data protection legislation permits disclosures for a number of reasons without consent, these include:

- To safeguard national security.
- The prevention or detection of crime, including the apprehension or prosecution of offenders.
- The assessment or collection of tax duty.
- The discharge of regulatory functions (includes health, safety and welfare of persons at work).
- To prevent serious harm to a third party.

- To protect the vital interests of the individual, this refers to life and death situations.

It is the responsibility of employees to ensure that they have the authority to share information, supported by appropriate documentation, and that the recipient is authorised to receive such information. All disclosures must be specifically authorised and recorded by the Corporate Assurance Section. Failure to do so could lead to action under the Service Disciplinary Policy (and in exceptional circumstances, criminal charges). The Service has a framework in place to facilitate information sharing with a wide range of local organisations, through the Humber Information Sharing Charter.

Advice should always be sought from the DPO if there is any uncertainty around the disclosure of information.

11. DATA TRANSFERS

Exports of data to countries outside of the UK (referred to in the UK GDPR as 'third countries') can only take place if an appropriate 'level of protection for the fundamental rights of the data subjects' are in place.

This means the transfer of personal data outside of the UK should only take place if one or more of the specified safeguards, or exceptions, apply:

- An adequacy decision
- Binding corporate rules
- Model contract clauses
- Legally binding and enforceable instrument between public authorities or bodies.

Exceptions: in the absence of the above, a transfer of personal data to a third country or international organisation, shall only take place on one of the following conditions:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers to the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the data controller or, the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12. CONSENT

The Service understands ‘consent’ to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be valid.

As a public authority and an employer, the Service hold a position of power over individuals so it is unlikely that consent will be deemed to be freely given. HFRS should only rely on Consent where no other condition exists.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The data controller must be able to demonstrate that consent was obtained for the processing operation in accordance with the Privacy and Consent Policy Delivery Guidance. For special category data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Where the Service provides information society services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

Whether or not a photograph or recording need to be protected or whether it falls under data protection legislation can be open to interpretation. However, the Service takes this matter extremely seriously and will always seek to obtain consent for photographic or recorded images to be used and/or published.

13. PROCESSORS AND CONTRACTS

The Service will ensure that it has a written contract or agreement in place with any processor it engages. This is important so both parties understand their responsibilities and liabilities. Processors must only ever act on documented instructions. To be compliant with data protection legislation, contracts must include specific items.

14. RETENTION AND DISPOSAL OF DATA

The Service will not keep personal data in a form that permits identification of data subjects for longer than is necessary, in relation to the purpose(s) for which it was originally collected. It may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in Service retention schedules.

Appropriate procedures must be followed when disposing of personal information. The Service will ensure that secure disposal methods are available to staff.

For further guidance, refer to the Disposal and Destruction of Records Policy Delivery Guidance.

15. RECORDS OF PROCESSING

Corporate Assurance will ensure that Records of Processing Activity (ROPA) are in place across all Service teams. These records of processing activity will complement the Information Asset Registers (IAR) and help determine the flow of data through the organisation. The Service is aware of any risks associated with the processing of particular types of personal data and the level of risk to individuals associated with the processing of their personal data.

The IAR/ROPA will be updated when necessary but will be fully reviewed at least annually by respective Information Asset Owners.

16. IMPACT ASSESSMENTS

The Service will implement technical and organisational measures to ensure that by default, personal data is processed were necessary. Data Protection Impact Assessments (DPIAs) will be carried out in relation to the processing of personal data, and in relation to processing undertaken by other organisations on behalf of the Service. DPIAs will be carried out in line with the Service's Data Protection Impact Assessment Policy Delivery Guidance.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, presents a risk to the rights and freedoms of an individual, the Service, prior to the processing, will carry out a DPIA. A single DPIA may not be required for each processing activity but may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA, it is clear that the Service is about to commence processing of personal data that could cause damage and/or distress to the data subjects or is deemed high risk (including to the reputation of the Service) the DPIA must be escalated for review to the DPO. The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

17. INCIDENTS AND BREACHES

The Service will always treat any data protection incident/breach as a serious issue. In the event of a breach, or suspected breach (incident), the Corporate Assurance Section must be informed immediately.

An investigation will take place in line with the Service's Personal Data Breach Notification Policy Delivery Guidance. This guidance involves Human Resources to ensure any disciplinary action is taken if deemed appropriate and Legal Services. The point of contact for the ICO is the Corporate Assurance Section.
The Service has an obligation to report certain data protection breaches to the ICO within 72 hours of the Service becoming aware of the event. The Corporate

Assurance Section will be responsible for notifying the ICO following an assessment of the breach. If required, the Corporate Assurance Section will also arrange for the affected data subjects to be notified. Any data processors the Service is working with are also required to report data protection breaches to the ICO, as well as cooperate with the ICO to resolve the issue. Data processors must also notify the Service of any breach which affects the Service's personal information, within the same 72 hour window.

The ICO has the authority to sanction significant financial penalties of up to £17.5 million. Data processors also hold liability for data protection breaches.

The Service recognises data subjects' right to compensation if they have suffered material or non-material damage as a result of an infringement of data protection legislation. Any claim for compensation will be dealt with through the Service's normal procedures.

18. RISK MANAGEMENT

As part of the Service's approach to risk management, all staff must adhere to the Policies and Guidance listed at Section 4 above.

19. TRAINING

It is the Service's policy that all employees and processors who have access to personal data held by the Service receive appropriate training, in order that they comply with data protection legislation. The Service will accordingly ensure that data protection training is available for staff.

Training in data protection matters should be provided before any access to personal data is permitted, and mandatory refresher training should be undertaken biennially thereafter to maintain awareness. Corporate Assurance are responsible for ensuring appropriate training is conducted periodically and monitor completion, including by temporary or contracted staff.

Data protection training is a crucial element of staff awareness. All individuals need to be aware of their obligations relating to any personal data they process as part of their Service duties. Failure to adhere to this policy can result in serious misconduct and lead to the prosecution of employees.

20. OUTCOMES AND IMPACTS

This Policy and its related guidance are designed to:

- Prevent the inappropriate use of personal data held by the Service.
- Ensure employees are aware of their responsibilities for handling personal data and that failure to do so could result in disciplinary proceedings, and in some cases criminal proceedings.
- Ensure services and employees know who to contact for advice.
- Training requirements are identified, and staff have the required level of data protection knowledge.
- Uphold data subjects' rights.

- Data processors working on behalf of the Service are aware of their responsibilities and handle personal data in accordance with this policy.
- Ensure the Service has an appointed Data Protection Officer, and their duties are defined.
- Ensure the Service is compliant with data protection legislation.

If anyone requires any further guidance / information relating to this document, please contact Corporate Assurance

APPENDIX A: APPROPRIATE POLICY DOCUMENT

1. Scope

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an appropriate policy document to be in place when processing special category and criminal offence data under certain specified conditions.

In order to operate effectively, Humberside Fire and Rescue Service (HFRS) has to process personal information which is listed in Schedule 1 of the DPA 2018. Almost all of the conditions in Schedule 1 of the DPA 2018, require an Appropriate Policy Document in place.

HFRS is committed to demonstrating that its processing of Schedule 1 conditions is compliant with the requirements of the UK General Data Protection Regulation (UK GDPR) Article 5 principles. This Appropriate Policy Document therefore complements the Service's record of processing under Article 30 of the UK GDPR and provides special category and criminal offence data with further protection and accountability.

2. Description of Processing Which Requires an Appropriate Policy Document

Schedule 1, Part 1 – Conditions relating to employment, social security and social protection.

Employment, social security and social protection

- Processing personal data concerning health in connection with our rights under employment law.
- Processing data relating to criminal convictions under article 10 UK GDPR in connection with our rights under employment law in connection with recruitment, discipline or dismissal.

Schedule 1, Part 2 – Substantial Public Interest Conditions

Statutory etc. and government purposes

- Fulfilling the service's obligations under UK legislation for the provision of services to residents of the geographic area served by the Humberside Fire Authority, that is the East Riding of Yorkshire, Kingston upon Hull, North Lincolnshire and North East Lincolnshire.
- Complying with other legal requirements, such as the requirement to disclose information in connection with legal proceedings.
- We may also process criminal offence data under this condition.

Equality of opportunity or treatment

- Ensuring compliance with the service's obligations under legislation such as the Equality Act 2010.
- Ensuring that we fulfil our public sector equality duty when carrying out our work.

- Ensuring we provide equal access to our services to all sections of the community in recognition of our legal and ethical duty to represent and serve communities.

Preventing or detecting unlawful acts

- Processing data concerning criminal records in connection with employment in order to reduce the risk to the Service and the community.
- Carrying out enforcement action in connection with the Service's statutory duties.

Protecting the public against dishonesty etc.

- Processing data concerning dishonesty, malpractice or other improper conduct in order to protect the local community.
- Carrying out enforcement action in connection with the Service's statutory duties.
- Carrying out investigations and disciplinary actions relating to our employees.
- Regulatory requirements relating to unlawful acts and dishonesty etc.
- Complying with the Service's enforcement obligations under UK legislation.
- Assisting other authorities in connection with their regulatory requirements.

Preventing fraud

- Disclosing personal data in accordance with arrangements made by an anti-fraud organisation.

Support for individuals with a particular disability or medical condition

- To provide services or raise awareness of a disability or medical condition in order to deliver services to service users.

Counselling

- For the provision of confidential counselling, advice or support or of another similar service provided confidentially.

Safeguarding of children and individuals at risk

- Identifying individuals at risk while attending emergency incidents.
- Obtaining further support for children and individuals at risk by sharing information with relevant agencies.

Insurance

- Information that is necessary for insurance purposes

Occupational pensions

- Fulfilling the Service's obligation to provide an occupational pension scheme.
- Determining benefits payable to dependents of pension scheme members.

Schedule 1, Part 3 – Additional Conditions Relating to Criminal Convictions, etc.

- The Service may process criminal conviction data in connection with child indecency offences.
- The Service may process personal data relating to criminal convictions in connection with its Service obligations or as part of recruitment and employment checks to protect the public against dishonesty.

3. Data Protection Principles

Article 5 of the UK GDPR states that personal data shall be:

- processed lawfully, fairly and transparently
- collected for specific and legitimate purposes and processed in accordance with those purposes
- adequate, relevant and limited to what is necessary for the stated purposes
- accurate and, where necessary, kept up to date
- retained for no longer than necessary, and
- kept secure

In addition, article 5 requires that the data controller shall be responsible for, and able to demonstrate compliance with, these principles (the accountability principle).

Processed lawfully, fairly and transparently

- the Service provides clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notices and policy documents.
- our processing for purposes of substantial public interest are necessary to exercise our functions which are outlined in legislation.
- our processing for the purposes of employment relates to our obligations as an employer.
- we also process special category personal data to comply with other obligations imposed on the Service in its capacity as a public authority e.g. the Equality Act.
- we carry out data protection impact assessments to ensure processing is fair and lawful.

Collected for specific, explicit and legitimate purposes

- We process personal data for purposes of substantial public interest as explained above when the processing is necessary for us to fulfil our statutory functions, where it is necessary for complying with or assisting another to comply with a regulatory requirement, to establish whether an unlawful act or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts or for disclosure to elected representatives.
- We are authorised by law to process personal data for the purposes outlined above.

- We process personal data only when it is necessary and proportionate.
- If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose. We implement data sharing agreements using the Humber Information Sharing Charter.
- We will not process personal data for purposes incompatible with the original purpose for which it was collected. If we do use personal data for a new purpose that is compatible, we will inform the data subject first.

Adequate, relevant and limited to what is necessary for processing

- We collect personal data necessary for the relevant purposes and ensure it is not excessive.
- The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Accurate and kept up to date with every effort to erase or rectify without delay

- Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. The Service has processes in place to help people do this.
- If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Kept in a form such that the data subject can be identified only as long as is necessary for processing.

- All data processed by the Service, unless retained longer for archiving purposes, will be retained for the periods set out in our retention schedules. The requirement for retention schedules is outlined in our Records Management and Data Quality Policy.
- We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.
- Our retention schedule is reviewed regularly and updated when necessary.
- We anonymise data when possible and this is covered in our training program.

Processed in a manner that ensures the appropriate security

- The Service will carry out risk assessments taking into account state of the art technical measures, the costs of implementation and the risk/likelihood to individuals if a security breach occurs and the effect of any security breach on the Service itself.
- Both the Service and its processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

- When assessing appropriate organisational and technical measures, IAOs and the DPO will consult with other relevant services, such as Digital Services, Human Resources and Audit.
- We adhere to the Government's Minimum Cyber Security Standards and implements information security controls in line with Public Sector Network, Payment Card Industry and Data Security Protection Toolkit. We also follow the guidelines of ISO27001.
- Employees working with or accessing data on vulnerable clients are subject to a Disclosure and Barring Service (DBS) check as described in our Safeguarding Policy and Disclosure and Barring Service Policy.
- All of our staff are trained in data protection matters and our contracts include confidentiality clauses.
- Technical security controls such as encryption are employed to secure sensitive information within systems.
- Role-based access controls are implemented to restrict access to sensitive data.
- Where possible, anonymisation or pseudonymisation are used to reduce the risk of sensitive data being compromised.

Accountability principle

- The Service has an information strategy in place which includes a protection policy and adheres to relevant codes of conduct.
- The appointment of a Data Protection Officer who reports directly to our highest management level.
- Taking a 'data protection by design and default' approach to our activities.
- Maintaining documentation of our processing activities.
- We have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing.
- Regularly reviewing our accountability measures and update or amend them when required.
- Having a well-established Corporate Assurance Team responsible for coordinating and monitoring compliance.
- All staff are routinely trained in key areas, including Data Protection.

4. Additional special category processing

The Service processes special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data, including our lawful basis for processing, in our privacy notices.

5. Evaluation

This Appropriate Policy Document will be subject to an annual review to ensure that it matches service delivery and the information being processed by the Service.