TITLE: DATA PROTECTION & CONFIDENTIALITY POLICY

1. INTRODUCTION

This policy sets out Hull City Council's approach to handling the personal information of identifiable living persons. It is designed to ensure we comply with our legal obligations, notably the General Data Protection Regulation 2016 (GDPR), Data Protection Act 2018 (DPA) and the Human Rights Act 1998 (HRA). An extended list of information legislation that governs the handling personal information can be found at **Appendix B.**

This policy is designed to ensure that our employees, Elected Members and other parties acting on our behalf understand their obligations when handling personal information and comply with the GDPR and DPA. Where customers, staff or partners require more detailed support or guidance, they should contact the Information Governance Team. A glossary of the terms used within the GDPR/DPA and this policy can be found at **Appendix C.**

This Policy is maintained by the Information Governance Team, Town Clerk's Service, email Information@hullcc.gov.uk

2. STATEMENT OF POLICY

Hull City Council needs to collect information about the people it works with in order to carry out its functions and deliver services to our residents. Hull City Council through its policy, procedures and training will make all efforts to:

- Comply with the law and good practice.
- Respect individual's rights and protect their privacy.
- Be open and honest with people about the data we hold.
- Ensure employees handling personal data have training and support that allows them to act confidently and consistently.

At the heart of data protection is the need to protect people's personal information and treat it with respect. Where the Council collects and uses personal data it will strive to work in accordance with the 6 data protection principles of the GDPR/DPA, these are listed at **Appendix A**.

The GDPR provides individuals with expanded rights over how their personal information is processed and these can be found at **Appendix E**. Where a data subject approaches the Council wishing to exercise any of these rights the request must be passed immediately to the Information Governance Team at Information@hullcc.gov.uk.

3. SCOPE

The policy applies to all employees of the Council including agency staff, contractors, any others employed under a contract of service and volunteers. The policy also applies to Elected Members in their role as a Member of the Council. This policy does not apply to Elected Members where they process personal data for constituency or political purposes. This policy does not apply to schools with delegated powers, unless adopted by the Governing Body.

This policy governs the processing of all personal information relating to identifiable, living persons. This includes electronic, paper or other permanent formats or file systems holding information. The policy applies throughout the lifecycle of the information from the time it is created or arrives at the Council to the point it is either destroyed or preserved permanently within the City Archives at the Hull History Centre.

4. ROLES AND RESPONSIBILITIES

4.1 Members

All elected members are to be made aware of this policy and of their duties and responsibilities under the GDPR/DPA. Members must handle personal information in accordance with the six data protection principles.

When Members handle personal information for political purposes, such as canvassing, they are covered by their political party's policies and rules. When accessing personal information as a member of the Council, for example as a member of a committee, they are covered by the Council's data protection policy and its registration with the Information Commissioner (Registration no. Z6005621).

Each Member is individually responsible for the personal information they use in their constituency work. The Council registers all Members with the Information Commissioner's Office as a separate data controller for their constituency work. The Register of Data Controllers can be viewed on the Information Commissioner Office website www.ico.gov.uk.

The Information Governance Team can provide general advice to Members in respect of personal information they process for their constituency work.

4.2 Corporate Strategy Team (CST)

The Corporate Strategy Team will ensure the Council complies with its legal obligations as a data controller under the GDPR/DPA.

CST will approve the corporate framework for data protection and receive regular reports from the Information Governance Group. CST will ensure an appropriate member of staff is nominated to act as the Council's Senior Information Risk Owner (SIRO)

4.3 Information Governance Group

The Information Governance Group will co-ordinate and oversee activity through regular meetings to ensure the Council meets its obligations to keep information safe, accurate and accessible.

The Information Governance Group:

- Will be chaired by the Council's Senior Information Risk Owner (SIRO).

- Will provide advice to service areas on developing service specific procedures and applying the Data Protection Policy.

- Will ensure that staff have received adequate data protection training and that adequate procedures and support are in place to allow them to comply with policies and the law.

- Will review and update the Data Protection Policy and procedures when legislative, technical or corporate changes occur;

- Will review information security breaches involving personal data to ensure risks are mitigated and, where necessary, escalated to CST.

- Will oversee and approve corporate Data Protection Impact Assessments.

The Information Governance Group will operate in accordance with its Terms of Reference.

4.4 City Managers

Each City Manager is accountable for data protection compliance within their service. They must ensure that their service complies with the principles of the GDPR/DPA when processing personal data. They must ensure that their staff are aware of their responsibilities under the GDPR/DPA and have received appropriate training. They will ensure that good Data Protection practice is established and followed by:

- Ensuring that appropriate staff are appointed as Information Governance Representatives who will assist with subject access requests and other information rights issues **(see Appendix I)**.

- Ensuring employees, including contractors, consultants and volunteers employed to undertake Council business have read and understood the data protection policy and guidance and have completed the e-learning testing **before** they are given access to customer data.

- Addressing any additional training needs for their service in the areas of privacy, confidentiality or security.

- Ensuring appropriate resources are in place to enable their staff to comply with the data protection policies and procedures.

- Notifying the Information Governance Group of any areas of information risk as they are identified.

- Reminding their staff that information security incidents involving personal information must be reported immediately **(see Appendix F)**.

4.5 The Information Governance Team

The Information Governance Team is responsible for:

- Maintaining the Data Protection Policy.
- Briefing senior managers on data protection responsibilities.
- Providing guidance and advice to staff on data protection issues, for example support writing privacy statements and information sharing agreements.
- Notification with the Information Commissioner's Office.
- Handling subject access requests (except social care see **Appendix G**).the Data Protection Subject Access Request Form is available on the intranet.
- Approving, in consultation with the Monitoring Officer and SIRO, unusual or controversial disclosures of personal data (for instance as part of Freedom of Information requests).
- Providing advice and assistance in the completion of Data Protection Impact Assessments where new or changed processing of personal information is under consideration.
- Supporting service areas in developing information sharing agreements in accordance with the Humber Information Sharing Charter.
- Recording and investigating information security incidents.

4.6 Data Protection Officer

The Data Protection Officer will:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise upon data protection impact assessments; train staff and conduct internal audits.
- Act as the first point of contact for supervisory authorities and for individuals whose data is processed.

4.7 Other specific staff

4.71 Information Security Management

The Assistant City Manager responsible for ICT networks is accountable for electronic information security including access to electronic systems and personal information stored on the Council's networks.

4.72 Corporate Procurement & Legal Services

The Council has standard wording in tender documents and contracts which require parties to comply with the requirements of the GDPR/DPA. The Procurement Team and Legal Services will ensure that additional contractual conditions are included where they are needed to ensure data protection compliance. More specific data handling or processing requirements must be included in contracts or appendices, or contracts must make provision for separate data handling and processing protocols. In most cases parties commissioned or contracted to deliver social care services will also be required to complete the NHS Digital Data Security and Protection Toolkit.

4.73 Caldicott Guardians

A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. The Guardian plays a key role in ensuring that the Council and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardians actively support work to enable information sharing where it is appropriate and advise on options for lawful and ethical processing of information. Their remits covers all social care records for children and adults.

As they have responsibilities relating to confidential information and information sharing, the Caldicott Guardians also have a strategic role, which involves representing and championing Information Governance requirements and issues at management team level and, where appropriate, at a range of levels within the organisation's overall governance framework. The Council's Caldicott Guardians are members of the Information Governance Group.

The Caldicott Guardian ensures that where confidential personal information is shared, for example with local NHS or other care partners, this is done properly, legally and ethically in line with the Caldicott principles.

4.74 Managers

All managers must ensure the people they manage have the necessary skills and knowledge to perform their duties. Managers must ensure that all their staff accessing personal information, including paper or other manual records, have read and understood the Data Protection Policy and associated guidance and completed the online Data Protection testing.

Managers must ensure that where new staff will have access to Council computer networks, or access to personal data held in non-electronic formats, that the new starter has read and understood the Data Protection Policy and guidance and has completed the relevant e-learning packages. A record of completion must be kept in the new starter's induction records.

4.75 All Staff

Intentional breaches of this policy will be handled under the Council's disciplinary procedures. If criminal activity is identified or reasonably suspected, the matter will be reported to the police and/or the Information Commissioner's Office.

All employees are individually responsible for complying with the GDPR/DPA. Maintaining confidentiality is also a requirement of all Council contracts of employment. Unauthorised access to, use of, or disclosure of personal data is a criminal offence under Section 170 of the DPA 2018. For example, viewing a person's file you have no business need to look at will breach the DPA, your contract of employment and the Council's policies. Disclosing personal information learned at work to a third party without the Council's permission will also breach the DPA and your contract of employment.

Where it is suspected that an employee has intentionally breached the GDPR/DPA the Council will report the details to the Information Commissioner's Office. It is considered unlikely that ICO will ever prosecute individuals for honest mistakes but they actively prosecute those who wilfully or recklessly access or disclose data where it is clearly wrong to do so.

Any unauthorised use, unauthorised disclosure or inappropriate access to personal information held by the Council will be dealt with under the disciplinary procedures. Any Council employee who wilfully and deliberately breaches this Policy and the GDPR/DPA should expect to be dismissed. The details will also be reported to the ICO and/or the Police and the Council will fully support any prosecutions.

5. SERVICE AREA AND CORPORATE PROCEDURES

From this policy and appendices, additional procedures and guidance may need to be developed. Each service will need to consider what specific guidance it must have in place in order to follow the data protection principles. Staff should exercise extra caution whenever their day-to-day work may impact upon how we process personal information, including:

- How we collect it.
- How much we collect.
- What we do with it.
- Whether it can be used for a new or changed purpose.
- How/where we store it.
- How we keep it secure.
- How we share it.
- Who we share it with inside the Council.
- Who we share it with outside the Council.
- How we respond to subject access requests.
- How we respond to official information requests from Police, HMRC, DWP etc.
- How we dispose of it.

Should advice or assistance be required the Information Governance Team should always be contacted for advice and assistance at the earliest opportunity.

5.1 How to process or use personal data

The definition of processing (using) data is very broad in the GDPR/DPA. Doing anything with personal data is likely to count as ‘processing’ under the Act. When Officers and Members need to use personal information they must ensure it is done lawfully and fairly (this is the first Data Protection Principle).

The main requirements for processing personal information are that we meet one or more of the conditions listed at **Appendix D** of this policy and that the processing can be considered to be ‘fair’. Wherever possible the Council must be clear when it collects personal information what purpose(s) it has been collected for, and all subsequent uses must be compatible with these conditions.

Wherever possible we must process personal information with the full knowledge of the data subject and this is most easily done by providing effective privacy notices at the point the information is collected. Services may contact the Information Governance Team for help writing simple and straightforward privacy notices for application forms, web forms etc. This will ensure individuals are clearly informed about how their information will be used in the future which will help avoid customer complaints and dissatisfaction.

Steps to take, and some to avoid, in the processing of personal information:

Do:

- Handle other people’s personal data with the same care and respect you would give your own information.
- Be particularly careful about sensitive ‘special category’ data concerning race, political opinion, religious belief, trade union membership, physical or mental health, sexual life, criminal offences.
- Wherever possible, tell people you hold personal data about them and explain why you need it, how long it will be kept, who you will share it with and who to contact for more information.
- Ensure personal data is kept accurate and up to date.
- Be very careful about passing personal information to third parties.
- Consult the Information Governance Team before using personal information for any new or significantly changed purposes – we may be required to complete a Data Protection Impact Assessment.
- Ask questions to confirm the identity of people who call you on the telephone before discussing personal details with them.
- Always use the minimum level of information necessary to get the job done, for example, do not take a full file out of the office if you only need to take a few pages or one section.
- Use lockable bags when taking sensitive paper records outside the office and ensure there is a return address/telephone number on the case.
- Review personal data kept in files often.

- Remember, emails may be revealed to those about whom they are written - any unprofessional or embarrassing comments you write about customers or colleagues will normally have to be disclosed to them upon request.
- Make Outlook calendar items containing personal information private by clicking on the padlock icon.
- Always double check correspondence before sending it – ensure envelopes are properly addressed and don't contain any unwanted items, ensure email addresses and any attachments are correct.
- Use secure email when sending personal information outside the Hull City Council email system (**Appendix H**).
- Direct any official requests to see personal data to the Information Governance Team at Information@hullcc.gov.uk.
- Consult your manager or the Information Governance Team if you are unsure whether to use, disclose or delete personal data.
- Report known or suspected information security breaches immediately to the Information Governance Team (**Appendix F**).

Don't:

- Use personal information if you are not sure it is appropriate – always ask your manager or the Information Governance Team for advice.
- Use personal data collected for one purpose for other reasons unless you have a clear legal basis and have established whether the data subjects should be provided with a new privacy notice.
- Reveal personal data to third parties without the data subject's permission unless there is a clearly established legal basis for sharing.
- Disclose any personal data over the telephone unless the caller has been properly identified.
- Leave personal data unsecured, (physical documents or electronic information) – You must keep a clean desk, lock confidential records in desks or cabinets and lock your computer when you move away from it.
- Share system passwords - you will be held accountable for any activity on Council systems that happens under your log in.
- Take personal data home or remove it from the Council's computer network unless you have a valid business need to do so and the data is appropriately protected, also you must have the explicit permission of the manager who is responsible for the data.
- Leave Council laptop computers or paper records in vehicles overnight – you must take them indoors and lock them safely away.
- Place or create Council information on personal electronic devices or personal email accounts, this is not permitted in any circumstances.

- Discuss confidential work matters with family, friends or anyone else outside work.
- Open suspicious emails and always report them via the service desk - if you click on an attachment or web link in an email and then realise it may be malicious it is important that you inform the Service Desk immediately. Disciplinary action will not be taken against any person who makes an honest mistake so please report any incident as quickly as possible.

5.2 How to keep personal information (records management)

The GDPR/DPA places a duty on organisations to keep personal information accurate and up to date. The Council's Records Management Policy provides guidance on how the Council manages its records and provides retention guidelines so our information is up to date and not held longer than necessary.

In accordance with the corporate Records Management Policy, City Managers have a responsibility to review their service's procedures and ensure they are keeping accurate and consistent records. In doing so, they will take the necessary steps to ensure any personal data held or processed by their service is accurate and is stored securely in accordance with the GDPR/DPA. The following are some of the actions that may be required to make sure data is stored accurately and is up to date.

5.21 Updating

Each service, as part of their responsibilities under the Records Management Policy will have processes for regularly checking and updating records and discarding old data.

5.22 Storage

In most cases, keeping personal information under lock and key is sufficient to meet the requirements of the GDPR/DPA. However, sometimes, extra security measures may be considered necessary.

5.23 Retention periods

Different records will have different retention periods. To comply with the fifth data protection principle the Council must make sure it has clear retention periods for the various types of personal information it holds. Retention periods can vary widely between document types. Please refer to the Council's Retention Schedule and electronic Information Asset Register on the Intranet for more details.

5.24 Disposal

If personal information is to be disposed of, this must be done securely. City Managers must ensure their services have appropriate arrangements in place for the disposal of personal or otherwise sensitive information. The Council's Facilities Management Team can provide advice on the secure disposal of personal and confidential information.

5.3 How to keep personal information secure

The Council must take all reasonable measures to ensure that personal information is kept safe and secure. Whenever personal information is collected, stored or transferred

appropriate measures must be taken to protect it. This may require encrypted and password protected devices, use of secure email or ensuring cabinets containing paper files are kept locked. **Appendix H** provides guidance on transferring data safely.

Employees, elected members or others acting on behalf of the Council must only collect, access and use the minimum level of information needed to properly carry out their duties and responsibilities.

Further guidance on keeping personal information secure will be provided through service specific training and through online training packages. Staff must also be aware of the relevant sections of the ICT Information Security policies which are designed to safeguard all information, not just personal data.

5.4 Data Breaches – What to do if something goes wrong

On occasion, personal data may be lost, stolen, or compromised. When this happens the incident must be reported **immediately**. This is vitally important as people may be put at risk of harm and quick action can reduce the potential for damage and distress to the victims (see **Appendix F**). The Council may also need to report the breach to the ICO within 72 hours.

A data breach is any incident involving the loss, damage, inappropriate disclosure or inappropriate access to Council information or unauthorised access to Council data systems. Such incidents can lead to identity fraud or have other significant impacts upon individuals and must be treated very seriously. A data breach can involve electronic or paper records or the verbal disclosure of details held in our systems or records.

Incidents must be reported immediately using Assyst or by contacting the Information Governance Team on 01482 613378 or Information@hullcc.gov.uk

All of the following should be reported as potential information security incidents:

- Human errors, for example sending letters or emails to the wrong address or selecting the wrong email attachment or putting the wrong letters in envelopes.
- Loss or theft of equipment containing personal information - laptops, mobile phones, USB drives, external hard drives, DVDs etc.
- Computer failures putting data at risk of loss, damage or being inaccessible for long periods.
- Breach of policies, e.g. employees looking at records they do not need to see or discussing confidential matters outside work.
- Computer hacking attack where third parties attempt to access our systems without permission.
- Failure to properly protect information, e.g. a file is left on the bus or a confidential email is sent without using the secure email system.
- A ‘blagging’ attack where somebody tricks us into releasing information;

- Any other incident where information is not kept safe or is used in a way that may be in appropriate.

If as a result of an incident you have concerns for any person's immediate safety you must try to warn them straight away.

Depending on the circumstances you may also wish to consult the Police - for example if the address of a person fleeing domestic violence has been disclosed to the perpetrator.

All incidents should be reported to the Information Governance Team **immediately** once they are discovered (see **Appendix F**). It will normally be appropriate to notify the service manager and/or City Manager particularly if there may be serious consequences for victims or if the incident is likely to attract publicity.

In deciding how to proceed consider the following:

- What data is involved?
- How sensitive is it?
- What format is it in and is it encrypted or otherwise protected?
- Who are the affected individuals?
- What could be the impacts on them?
- Are there any things we can do right now to recover the information or limit impact on the victims?

Any 'near-miss' situation (data was not compromised, lost or stolen but nearly was) must also be reported for investigation. It is vital that all employees play their part in protecting information and make their manager and the Information Governance Team aware of any risks they identify.

It is not the Council's policy to pursue serious disciplinary action against employees who make genuine human errors but any failure to report an incident will be treated extremely seriously.

5.5 Requests for copies of personal data (Subject Access Requests)

Under the GDPR/DPA any person has a right to ask for a copy of their personal information from any organisation. When someone requests their own information, this is called a Subject Access Request (SAR). The Council must provide any information it holds within 30 calendar days. There are some limited exemptions from this right of access but in most cases all information must be provided.

It will not always be appropriate to use the SAR process. For example, if a customer asks how much Council Tax they owe or for the balance of their rent account this should be dealt with as a normal service request. However, if a customer requests a copy of all information the Council Tax Team holds about them or a full copy of their Housing file this should be dealt with as a Subject Access Request and passed to the Information Governance Team.

Where a customer asks for a copy of their personal information they should be directed to the Subject Access Request form (**Appendix G**) on the Council's website or advised to contact 300300 or the Council's Information Governance Team. If the customer wishes to

make a verbal request you should record the details in writing, including their preferred contact details, and forward it to the Information Governance Team.

If you are unsure how to deal with a request for information please contact the Information Governance Team who can advise you on the appropriate response.

Written requests for information which do not include the applicant's own personal data will be handled in accordance with the Freedom of Information Act. All such requests should be forwarded to the Information Governance Team.

5.6 Sharing personal information with a partner organisations

Information sharing is vital to the Council's ability to deliver better, more efficient public services that are coordinated around the needs of our customers. It is essential to enable early intervention and preventative work and in some cases for safeguarding and public protection.

At the same time, the Council acknowledges that the public want to be confident that their personal information is kept safe and secure. Council officers must maintain a balance between the privacy of individuals, operational requirements and the law.

Council staff making decisions about information sharing must do so on a case-by-case basis, the checklist at **Appendix J** outlines considerations for sharing in accordance with the GDPR/DPA. In cases where there is a regular exchange of personal data the Humber Information Sharing Charter should be used to agree the sharing.

5.7 New projects or systems involving personal information

Any new uses of personal information must be assessed to ensure they are lawful and will not put personal data at risk. Any new, or significantly changed, use of personal information must be assessed and where appropriate a Data Protection Impact Assessment (DPIA) must be completed. The Information Governance Team can provide assistance in completing a DPIA before they are submitted to the Information Governance Group for feedback and approval.

6. TRAINING AND AWARENESS

All staff and Councillors will need to be aware of the Council's Data Protection & Confidentiality Policy. Employees with access to Council ICT and data systems are required to complete annual data protection training on Oracle Learning Management. For some posts additional training and guidance will also be provided within the service.

6.1 Induction

When staff and Councillors join the Council, it is important that they are introduced to their basic responsibilities under the GDPR/DPA. For many staff and Councillors, this level of understanding will be met by reading this policy and completing the online training packages. However, staff may need additional awareness based upon any specific induction requirements within their service groupings.

6.2 Continuing training

If additional Data Protection training or awareness is required beyond this policy, staff should bring this to their manager's attention. If you require assistance with any particular data protection issue, please contact the Information Governance Team.

7. NOTIFICATION TO THE INFORMATION COMMISSIONER

Hull City Council is registered with the Information Commissioner's Office and is included on the public register of data controllers (Registration no. Z6005621).

Any changes to the register must be notified to the Information Commissioner within 28 days. For this reason any new processing of personal data must be brought to the attention of the Information Governance Team so Hull City Council's notification can be updated as necessary.

8. POLICY REVIEW

This policy will be reviewed at least once every three years and the appendices will be updated as necessary. This Policy is maintained by the Information Governance Team who may be contacted with comments and feedback at Information@hullcc.gov.uk

9. POLICY HISTORY

Policy History:

Implementation:
Updated:
Revised:
CJCNC: 7 September 2018

Appendix A

The Six Principles of Data Protection

The Council is committed to working in accordance with the Principles of Data Protection. These 6 Principles which form the basis of the GDPR/DPA are as follows -

1. The first data protection principle is that the processing of personal data must be lawful, fair and transparent.

2. The second data protection principle is that—

   (a) The purpose for which personal data is collected on any occasion must be specified, explicit and legitimate, and

   (b) personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected.

3. The third data protection principle is that personal data must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

4. The fourth data protection principle is that personal data undergoing processing must be accurate and, where necessary, kept up to date.

5. The fifth data protection principle is that personal data must be kept for no longer than is necessary for the purpose for which it is processed.

6. The sixth data protection principle is that personal data must be processed in a manner that includes taking appropriate security measures as regards risks that arise from processing personal data. These risks include (but are not limited to) accidental or unauthorised access to, or destruction, loss, use, modification or disclosure of, personal data.

Appendix B

Related Legislation

- Common Law Duty of Confidence
- The Human Rights Act 1998
- The Data Protection Act 2018
- The EU General Data Protection Regulations 2016
- Computer Misuse Act 1990
- The Freedom of Information Act 2000 (FOI Act)
- The Caldicott Report 1997
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- The Environmental Information Regulations 2004 (SI 2004/3391)

Appendix C

GLOSSARY

Processing – obtaining, recording or holding information or data, or carrying out any operation or set of operations on that information or data. This will include:

a) Collection, recording, organisation, structuring or storage,

(b) Adaptation or alteration,

(c) Retrieval, consultation or use,

(d) Disclosure by transmission, dissemination or otherwise making available,

(e) Alignment or combination, or

(f) Restriction, erasure or destruction,

Data Subject – any living individual who can be identified from the data, this data may not necessarily include their name.

Personal Data – "Personal data" means any information relating to an identified or identifiable living individual

Data Controller – person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

Note: The Data Controller is usually a company or organisation rather than an individual within that company or organisation.

Hull City Council is the data controller for all of the systems in use within this organisation and is registered with the Information Commissioner's Office.

'Special Category Data', also known as 'Sensitive Personal Data'

Extra care must be taken with the handling and use of special category data, for the purposes of this policy this is -

(a) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;

(b) The processing of genetic data for the purpose of uniquely identifying an individual;

(c) The processing of biometric data for the purpose of uniquely identifying an individual;

(d) The processing of data concerning health;

(e) The processing of data concerning an individual's sex life or sexual orientation;

(f) The processing of personal data as to —

(i) The commission or alleged commission of an offence by an individual, or

(ii) Proceedings for an offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings.

Appendix D

Conditions for Processing Personal Information

We must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing within the GDPR. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on our purpose and relationship with the individual. See below.

If we are processing special category data we need to identify both a lawful basis for general processing and an additional condition for processing this type of data. See below.

Most lawful bases require that processing is **'necessary'**. If we can reasonably achieve the same purpose without the processing, we won't have a lawful basis.

We must determine the lawful basis before we begin processing, and should document it. Take care to get it right first time - we should not swap to a different lawful basis at a later date without good reason.

Our privacy notice should include the lawful basis for processing as well as the purposes of the processing.

If our purposes change, we may be able to continue processing under the original lawful basis if the new purpose is compatible with the initial purpose (unless your original lawful basis was consent).

Conditions for processing personal data

GDPR Article 6 (1) states that
'Processing shall be lawful only if and to the extent that at least one of the following applies' –

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) Processing is necessary for compliance with a legal obligation to which the controller is subject;
d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Conditions for processing special category data

GDPR Article 9 states that -
Processing of personal data revealing 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 shall be prohibited unless –

a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) Processing relates to personal data which are manifestly made public by the data subject;
f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim

pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Processing on the basis of consent

The GDPR increases the standard for consent. The Information Commissioner's Office has made it clear that public authorities and employers, such as the Council, will find it very difficult to use consent as the basis for processing personal information. Where a service believes that consent is the appropriate basis for their processing personal information they must consult the Information Governance Team before collecting any information.

In many cases it will still be appropriate to obtain consent to deliver services, treatment or support but any such consent must not include consent to process personal information under the GDPR.

Services must ensure that privacy notices are issued to service users at the point personal data is collected and each notice must provide comprehensive information on how the data will be processed – the Information Governance Team provides advice and support writing privacy notices.

Appendix E

Individual Rights under the GDPR/DPA

There are eight data subject rights under the GDPR/DPA.

a) The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. We must provide individuals with information including: purposes for processing their personal data, retention periods and who it will be shared with. We call this 'privacy information'.

We must provide privacy information to individuals at the time we collect their personal data from them.

The information we provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

b) The right of access

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data and other supplementary information. It helps individuals to understand how and why we are using their data, and check we are doing it lawfully. Requests can be made in writing or verbally and in most cases no fee can be charged.

c) The right to rectification

Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve allowing the individual to attach a supplementary statement to the data.

This right has close links to the accuracy principle of the GDPR However, although you may have already taken steps to ensure that the personal data was accurate when you obtained it, this right imposes a specific obligation to reconsider the accuracy upon request.

d) The right to erasure

The GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing and we have one month to respond. The right to erasure is not absolute and only applies if –

- The personal data is no longer necessary for the purpose which we originally collected or processed it for;
- We are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;

- We are relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- We are processing the personal data for direct marketing purposes and the individual objects to that processing;
- We have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the GDPR);
- We have to do it to comply with a legal obligation such as a Court Order; or
- We have processed the personal data to offer information society services (social media) to a child.

The right to erasure does not apply if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation;
- For the performance of a task carried out in the public interest or in the exercise of official authority;
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- For the establishment, exercise or defence of legal claims.

The GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- If the processing is necessary for public health purposes in the public interest (eg protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- If the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

Requests for erasure must be passed immediately to the Information Governance Team.

e) The right to restrict processing

Individuals have the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction. This may be because they have issues with the content of the information you hold or how you have processed their data. In most cases you will not be required to restrict an individual's personal data indefinitely, but will need to have the restriction in place for a certain period of time.

Requests to restrict how we process an individual's data must be passed immediately to the Information Governance Team.

f) The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

The right to data portability only applies when:

- Our lawful basis for processing the information is consent or for the performance of a contract; and
- We are carrying out the processing by automated means (i.e. excluding paper files).

Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits. The right only applies to information an individual has provided to us.

g) The right to object

Individuals have the absolute right to object to the processing of their personal data if it is being used for direct marketing purposes. Individuals can also object if the processing is for:

- A task carried out in the public interest;
- The exercise of official authority vested in you; or
- Your legitimate interests (or those of a third party).

In these circumstances the right to object is not absolute.

There is also a more limited right to object to processing for scientific or historical research, or statistical purposes.

h) Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement); and
- Profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

  The GDPR has additional rules to protect individuals if we carry out solely automated decision-making that has legal or similarly significant effects on them. We can only carry out this type of decision-making where the decision is:

  - Necessary for the entry into or performance of a contract; or
  - Authorised by Union or Member state law applicable to the controller; or
  - Based on the individual's explicit consent.

  Where we undertake any automated decision making or profiling we must make sure that we:

1. Give individuals information about the processing;
2. Introduce simple ways for them to request human intervention or challenge a decision;
3. Carry out regular checks to make sure that our systems are working as intended.

More information can be found on the Information Commissioner's website at www.ico.gov.uk or by calling the Commissioner's Helpline on 0303 123 1113 (local rate) or 01625 545 745 (national rate).

Appendix F

Data Breach Procedures for Council Staff

All actual or suspected data breaches **(see 5.4 above)**, including 'near misses', must be reported as soon as they are discovered using the 'Information Security Incident' category on ASSYST or by emailing or calling the Service Desk. Alternatively you may contact the Information Governance Team by telephone or Information@hullcc.gov.uk

Each case will be assigned to an investigating officer who will in most cases be senior member of the service in which the breach occurred supported by a member of the Information Governance Team. The investigating officer will ensure the incident is contained, arrange for all necessary parties to be informed and ensure appropriate measures are taken to reduce the risk of similar incident in the future. In order to assist with this please provide the following when reporting an incident:

- What data is involved?
- What format it is in and whether it is encrypted or otherwise protected?
- Who is affected, what type of information and how many records?
- How sensitive is the information?
- Are there any potential risks to individuals?
- What steps have already been taken to recover/locate the information?
- If items have been stolen, please ensure the incident has been reported to the police and provide the crime number.
- What actually happened and which employees were involved?
- Details of any ongoing, immediate risk to information security.

If as a result of an incident you have concerns for any person's immediate safety you must make all reasonable efforts to warn them straight away.

Depending on the circumstances you may also need to think about consulting the Police - for example if the address of a person fleeing domestic violence has been disclosed to the perpetrator.

Appendix H

Transmitting Personal Information – Email, Post and Fax Other Methods

There are always risks associated with transferring personal information. Appropriate security must be used for every transfer in order to minimise risk. The severity and type of these risks will vary depending on the method of transfer. Examples of such risks include:

- Information being lost, damaged or intercepted in transit e.g. stolen laptops, lost memory sticks, opened envelopes
- Delivery service delivering mail incorrectly
- Information being sent to the wrong address via e-mail, post or fax
- Information received by the organisation but not delivered to the correct person
- Personal information not being disposed of appropriately
- Information that is deliberately transferred with criminal/fraudulent intent e.g. ID theft

Where personal information is compromised there may be an impact on the following:

- Individuals - whose information has been put at risk;
- Staff - whose actions placed the information at risk. Such staff may have breached local policy and this could potentially lead to disciplinary action. There may also be legal implications and potential criminal action taken if they have breached key legislation.
- Organisations - whose actions placed the information at risk.
  Such organisations may experience a lack of trust confidence or reputation from the public and potential prosecution under information legislation.

Guidelines for transferring personal information are included below however wherever an employee is unsure of the most appropriate method for transmitting personal data they should consult the Council's Information Governance Team. ICT may also be able to provide secure solutions for regular or bulk transfers of personal information.

Email – SFX and Secure Envoy Email Systems

Personal information may only be sent by Council email to another 'hullcc.gov.uk' email address. Where it is necessary to send personal or otherwise confidential information to an email address outside the Hull City Council network this must be done using a secure email tool.

Staff may not email Council information to their personal email accounts. However, staff may email their own personal information to themselves at their own risk, for example a copy of their online payslip, but they must not forward any information they have access to as part of their job to their personal email account.

If you regularly send personal information to a particular public sector organisation such as the NHS, Department of Work and Pensions, the Police or another Local Authority there may be more efficient ways to safely email between organisations. Contact the Information Governance Team using Information@hullcc.gov.uk if you need more advice on this subject.

Secure Envoy

Where there is a need to send personal information to an email account which is not on the Public Service Network, for example gmail or hotmail, this must be sent by SFX or the Secure Envoy system.
SFX can be accessed through the intranet - http://home.hullcc.gov.uk/my-job/tools/secure-email-file-transfer-sfx the recipient will need to log into the SFX secure website to access the information.
Alternatively you can contact the Service Desk to have the 'Send Secure' button added to your email account. The Secure Envoy system will send an encrypted email and it is necessary to agree a password with the recipient before the email is sent to them.

Post – Internal and External

Wherever possible documents should be scanned and the electronic copy sent by email or other secure electronic means.

Internal Post Services

Personal information sent by internal mail must always be in a sealed envelope and addressed to a named recipient. Where the information is sensitive, the envelope should be protectively marked.

Care should be taken when re-using envelopes to ensure any previous address is properly removed or obscured to avoid the correspondence being sent to the old address by mistake.

Where the contents relate to an employee's personal life rather than their work (for example occupational health issues or their pension) ensure the envelope is clearly marked 'Private & Confidential'.

External Post

Postal and courier services can be used to transfer personal information either in paper format or as electronic information on removable media.

An assessment of the risk posed by sending personal information by post or courier must always be carried out in order to decide whether it is appropriate to use these methods. The following should be considered and a senior manager consulted should there be any doubt:

- The nature of the information, its sensitivity, confidentiality or value.
- The damage or distress that could be caused to individuals if the information was lost or stolen.
- The effect any loss would have on the Council

There are a number of standard requirements which must be adhered to when transferring information by post or courier services:

- Confirm the name, department and address of recipient and enter details correctly on the envelope/parcel.
- Mark the envelope/parcel, private and confidential and add on return address details where this will not compromise confidentiality.
- Package securely to protect the contents from being tampered with or from any physical damage likely to arise during transit.
- Consider use of an approved courier, registered post or other secure mail method which can be tracked and is signed for.
- Electronic information on USB stick or hard drive being sent by post or courier, must be encrypted prior to transfer – consult ICT for advice in each case.
- Couriers must be made aware of the sensitivity of the contents and any delivery instructions – for example 'do not leave with neighbours' or 'return to sender if unable to deliver'. These instructions should be confirmed with the courier service in advance.

Fax

Always consider alternatives to faxing personal information - for example secure email or delivery by courier. **Fax should always be a last resort!**

Where it is absolutely necessary to fax personal information the following measures must be taken:

- Telephone the recipient of the fax let them know that you are about to send a fax containing confidential information.
- Ask if they will wait by the fax machine whilst you send the document.
- Ask if they will acknowledge the receipt of the fax.
- Check the fax number you have dialled and check again that it is correct before sending.
- If this fax machine is going to be used regularly, store the number in your fax machines memory.
- Request a report sheet to confirm that the transmission was O.K.
- Do not leave the fax on the machine when it has been sent.
- Make sure that you have clearly stated on the fax cover sheet that the information you are sending is confidential. Please see below for suggested wording.

Suggested wording for fax cover sheet:

The information contained in this fax is **STRICTLY CONFIDENTIAL** and intended for the named recipient only. If you are not the named recipient you must not copy, distribute or disseminate this information, nor disclose its contents to any person. If you have received this fax in error, please notify the sender immediately. Thank You

When sending personal information by fax you must not:

- Send faxes where you know that the information will not be promptly collected by the intended recipient
- Send faxes at times that maybe outside the recipient's hours of work
- Leave information unattended whilst a fax is being transmitted

Transporting Data by Hand (Paper and Electronic)

Wherever possible data should be transferred by secure electronic means such as secure email.

However, there may be occasions when it is necessary for an employee to transport information outside the Council 'by hand', whether in paper files or on a portable electronic device. In all such cases these rules must be followed:

- Wherever reasonably practical original files should not be removed from the Council's offices/systems - instead a copy of the original information should be taken.

- Only the minimum information necessary for the task may be transported. Copies of full files must not be used if only a small section is required.

- A record must be kept of all original documents which are taken outside the Council. Enough detail must be recorded to ensure we would know what had been lost if it went missing or was destroyed.

- Information should be de-personalised, as far as practical, in order to limit the damage if it were to be lost or stolen. Any details which are not necessary should be removed.

  For example, an officer making regular visits to vulnerable individuals may only need a list of the customers' initials and the time of each appointment rather than a print out titled 'Supported Housing Visits' with each customers' name, address, date of birth and telephone number.

- Any electronic device used to transport personal information must have been properly encrypted by the Council's ICT Service. As well as laptops, tablet computers and smart phones encryption must also be applied to storage devices such as portable hard drives and USB memory sticks. Please note that the use of a log on password or pin number does not necessarily mean that a device is encrypted. If you are unsure whether a device is appropriately encrypted please consult ICT immediately.

- Staff may not use their personal computer, mobile phone or any other electronic device to store or transport Council information without the written permission of their City Manager. Where the information contains personal data written permission must also be obtained from the Data Protection Officer. Where the information contains health and/or social care information written permission must also be obtained from the Council's Caldicott Guardian.

- Wherever practical, devices or records containing personal information should be returned to Council premises at the end of the working day rather than being take home by the employee.

- Where it is necessary for an employee to take a device or records home overnight they must make all reasonable efforts to keep them safe. They must be stored in a place which is out of sight to visitors; preferably in a locked cabinet or room. The employee must ensure the information is not accessed by any member of their household or person visiting their home.

- Staff using paper diaries or notepads which are taken outside Council premises must remove any personal information from them at the earliest opportunity. Any details which need to be retained should be moved onto the relevant paper file or computer system. If the original version is not to be retained on file it should be securely shredded.

- Where information must be transported by hand all reasonable security measures to protect it must be taken be taken, these should include as a minimum:

    - Devices or records must not be left unattended in public;
    - Devices or records should be transported in secure lockable bags;
    - When using public transport the employee must not leave the bag containing the records or electronic device unattended on luggage racks but should instead keep it with them; extra care should be taken to remember the bag when getting off the train, bus, hovercraft etc;
    - Devices or records should not be left in private vehicles but if it is unavoidable they must not be left where they can be seen – instead they should be locked in the boot or a lockable storage compartment.

- Any loss, theft or destruction of the information must be reported as an Information Security Incident at the earliest possible opportunity. The Council will treat any failure to report lost, damaged or destroyed personal information very seriously in accordance with its disciplinary procedures.

Appendix I

Information Governance Representatives

Role

- Act as the first point of contact for the Information Governance Team for Subject Access Requests
- Act as the first point of contact on data protection issues including information security incidents

Responsibility

- Signpost other staff within the service to the Information Governance Team
- Help locate personal information in order to answer subject access requests
- Co-ordinate their services' responses containing personal information to the Information Governance Team
- Aid the Information Governance Team with service specific knowledge in respect of information requests and decisions on disclosing or withholding information

The Information Governance Representatives also perform the same role for each service in respect of Freedom of Information requests.

Appendix J

Sharing Personal Information

1. **Remember that the GDPR/DPA is not a barrier to sharing information**

It provides a framework to ensure that personal information about living persons is shared appropriately.

2. **Seek advice**

If you are in any doubt seek advice about the proposed sharing. Contact the Information Governance Team if you have any questions.

3. **Be open and honest**

Let the person (and/or their family where appropriate) know from the outset why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

4. **Share with consent where appropriate**

Where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case. In such cases it is recommended that you consult the Information Governance Team or an appropriately qualified professional such as a social worker.

5. **Consider safety and well-being**

Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.

6. **Necessary, proportionate, relevant, accurate, timely and secure**

Remember that the data protection principles still apply. You will need to ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely. Do not provide details that are not needed or asked for!

7. **Keep a record of your decision to share information**

Remember to record the reasons for sharing whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Although these principles cover sharing of information with anyone or any organisation, staff should ensure that if they are sharing information on a regular basis with an organisation that they have a formal information sharing protocol in place.

If you are sharing or disclosing personal information to a third party, please ensure that you have proper authorisation to do so either as part of your normal working practice.

The Police may request information from the Council for the purposes of preventing or detecting crime, locally such requests may be marked ‘DP9’ or ‘Schedule 2 Part 1 5(3) of the Data Protection Act 2018’.

All requests from the Police should normally be referred to the Information Governance Team. Please pass any such requests to the Information Governance Team as quickly as possible.

If you are in any doubt whether you can share information or disclose it to a third party please contact the Information Governance Team before taking any action.