IPSWICH
BOROUGH COUNCIL

Data Protection Policy

Version number	Signed off by	Written/Amended by	Last Updated/Reviewed	Date of next review
V0.1		Suzy Valentine	March 2017	
V1.1		Senior Information Governance Officer	July 2019	July 2020
V1.2		Senior Information Governance Officer	June 2021	June 2024

IPSWICH BOROUGH COUNCIL DATA PROTECTION POLICY

The UK GDPR and Data Protection Act 2018 together form data protection law within the UK.

The law aims to protect the privacy of individuals, and to ensure that information about them is not processed without their knowledge nor used for a purpose they have not expressly agreed to, unless covered by an exception under the legislation.

The legislation covers personal data relating to living individuals (the Data Protection Act calls them Data Subjects) and classifies some personal particulars as special categories of personal data which attract more stringent standards of protection than ordinary personal data do.

Ipswich Borough Council (IBC) confirms that it is committed to protecting individuals' privacy by processing their personal data in accordance with this Policy.

1. Scope of the policy

1.1 The Data Protection Act 2018 (DPA 2018) and UK GDPR apply to all IBC's electronic and paper records held in structured filing systems containing Personal Data, as defined below. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to Personal Data held visually in photographs or video clips (including CCTV), to audio recordings and to data on its website. IBC possesses a large amount of Personal Data including employee records and references and processes a wide range of records containing names and addresses and personal details about a wide range of customers and service users.

1.2 The UK GDPR and DPA 2018 covers personal data, which is automatically processed, and certain manual data as defined below:

DATA is defined as "information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose" or information recorded as part of a "relevant filing system". This applies to all computer systems and most manual filing systems.
PROCESSING is obtaining, recording or holding information or data or carrying out any operation or set of operations on that information or data.
DATA CONTROLLER is someone who determines the purposes for which and the manner in which any personal data are or are to be processed. i.e. someone who collects it and controls its contents and use, in the present case, Ipswich Borough Council.
PERSONAL DATA is information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the Data Controller), including any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect to that individual. This covers data containing such information as addresses, telephone numbers, etc, as well as data containing actual names. It could also cover references by title if these are sufficiently specific e.g. Chief Executive, Head of Legal and Democratic services, IT Operations Manager. It also covers data that can be associated with an individual using other data in the data controller's possession e.g. if computer data had a works number as an identifier, but a manual file related the works number to the name of an individual, the personal data would still be covered by the law. **DATA SUBJECT** is an individual who is the subject of personal data. Every living person, therefore, is capable of being a data subject and in the case of IBC that could be its employees or individuals at third parties with whom it deals e.g. a project manager for a contractor undertaking some maintenance works.
RECIPIENT is defined as any person to whom personal data is disclosed (this includes employees of a data controller).
SPECIAL CATEGORY PERSONAL DATA is defined as data relating to:

a) the racial or ethnic origin of the Data Subject;
b) their political opinions;
c) their religious or philosophical beliefs;
d) whether they are a member of a trade union;
e) genetic data;
f) biometric data (where this is used for identification purposes);
g) their physical or mental health condition;
h) their sex life or sexual orientation.

CRIMINAL CONVICTION DATA is defined as data relating to:
a) the alleged commission of offences by the data subject;
b) proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing.

2. Organisational Responsibilities

2.1 The legislation means that IBC must:
- Manage and process personal data properly;
- Protect the individual's rights to privacy;
- Provide an individual with access to all personal information held on them.

2.2 IBC's Executive has responsibility for ensuring that IBC adopts a Data Protection Policy to ensure that IBC complies with the duties and responsibilities contained in the legislation. IBC is a corporate body, is named as the Data Controller under the DPA 2018. IBC acting through its Data Protection Officer is required to notify the Information Commissioner of the processing of personal data and this notification is included in a public register. The public register of data controllers is available on the Information Commissioner's website.

2.3 The Data Protection Officer is responsible for drawing up guidance on good data protection practice and promoting compliance with this guidance by advising staff. Where no specific guidance has been issued to staff, managers and staff are expected to follow the guidance from time to time issued by the Information Commissioner.

2.4 Each of the Heads of Service is responsible for ensuring that they put in place in their respective service areas procedures to ensure that any records (whether manual or electronic) containing Personal Data are managed and processed by their employees or any third-party contractors in a manner that is compatible with all legal requirements.

2.5 Operations Managers are responsible for ensuring compliance with service area procedures in line with the guidance set out in this document and as provided by the Data Protection Officer and for arranging for any necessary induction training for new employees.

2.6 Every member of staff who accesses information about identifiable living individuals is responsible for ensuring that they comply with good data protection practice and this policy.

2.7 The role of Data Protection Officer is carried out by the Audit Partnership Manager and Senior Information Risk Owner (S.I.R.O). Data protection compliance is managed by the Information Governance team within Legal and Democratic Services.

2.8 All staff are reminded that individual employees can also be held liable for breaches of the legislation.

2.9 IBC is committed to observing the six data protection principles in the course of processing personal data. The principles are that personal data should be:

a) processed lawfully, fairly and in a transparent manner,
b) collected for specified, explicit and legitimate purposes,
c) adequate, relevant and limited to what is necessary,
d) accurate and, where necessary, kept up to date,
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed and,
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In practical terms, this means informing the data subject of the data being processed from the outset, keeping the data secure and regularly evaluating the worth of retaining information and where it is no longer required, and with reference to appropriate timescales for document retention, disposing of it in a timely and secure fashion.

3. Data Subjects Rights

Data Protection law gives data subjects several legal rights. These are:

- **The right of access:** Individuals can ask the Council for a copy of the personal information it holds or processes relating to them. We should provide the information within 1 month. If there is a great deal of information or it is difficult to identify and retrieve, then we can ask for a time extension.
- **The right to rectification:** Everyone is entitled to have their own personal data rectified / changed if it is inaccurate or incomplete. If an organisation has shared the personal data in question with anyone else, then it must also take all reasonable steps to inform them of the change. Data subjects will be asked to provide

evidence of their identity and the correction so that the organisation can ensure their privacy rights are protected.

- **The right to erasure:** The right to erasure can sometimes be referred to as 'the right to be forgotten'. However, this is not an absolute right. Individuals can only request the deletion or removal of personal data where there is no compelling reason for an organisation to keep it. Where the organisation has a statutory obligation or a legally justifiable reason to keep the information they must let them know.
- **The right to restrict processing:** In some circumstances people have a right to restrict what processing an organisation carries out or ask that they stop processing their personal data. When processing is restricted, the organisation may continue to store the data but not to process it further. However, this right cannot overrule any legal obligation placed on the organisation to continue processing the personal information.
- **The right to data portability:** Following a request for disclosure of an individual's data, they have the right to ask for their information in a digital format so that they can reuse it for other purposes. For example, data portability could be used to upload information to a third-party price comparison website to compare and identify best value for something like utilities or mobile phone use. It is unlikely that data portability will apply to most of the services received from the Council.
- **The right to object:** Everyone has the right to object to the processing of their data in limited circumstances. However, they can only object based on "grounds relating to their particular situation". For example, they may need to maintain a higher level of security due to the type of job they have. In these situations, an organisation must stop processing the personal data unless it can demonstrate compelling grounds for the processing, which override an individual's interests, rights and freedoms or where processing is for the establishment, exercise or defence of legal claims.
- **Rights related to automated decision making and profiling:** Data subjects have a right to request that decisions based solely on automated processing, including profiling, which may produce a legal effect or affect them significantly, have some form of human input so they are not automatically generated by a computer. This right is in place to ensure that potentially damaging decisions are not taken without some form of human intervention. This right also applies to 'profiling'.

Further information on how data subjects can exercise their rights is available on the website at www.ipswich.gov.uk/privacy

4. Handling data inquiries and breaches

4.1 IBC will respond to requests from individuals to be provided copies of information held on them (a process the DPA 2018 dubs a subject access request) within the prescribed timescales. The council website

will provide advice to individuals on who to contact and how long it will take to provide the information.

4.2 In the event that an individual challenges a response to a request, IBC will, in the first instance, undertake an independent internal review of the original response. Where the data subject has escalated the complaint, IBC will comply with the requests of the Information Commissioner.

4.3 While IBC will strive at all times to observe good data protection practice, there may be occasions when a data breach occurs. Where this happens, IBC will act swiftly to contain the breach, mitigate any effects and conduct an investigation where necessary which may identify further training needs or disciplinary action required. Where necessary, IBC will notify the Information Commissioner.

5. Relationship with existing policies

5.1 This policy complements IBC's Freedom of Information policy.

5.2 Copies of the policies are held on the Council's Intranet and should be referred to when necessary. They will be reviewed and updated regularly.

6. IBC will strive to conduct regular audits of data protection practice to ensure compliance.