

DATA PROTECTION POLICY AND PROCEDURES 2025

Author	Louisa Godfrey
Date of implementation	09.09.23
Date of last review	30.01.25
Date of next review	30.01.26
Version Number	3
Location of most recent version	BRIGHT HR

Purpose Statement by the Company Director

In delivering its services Godfrey Group will need to collect and process certain types of information about people including company staff, clients and suppliers or providers of services to it. All such processing is subject to the General Data Protection Regulation (GDPR) and the more particularly the Data Protection Act 2018. This policy sets out Godfrey Group's intentions in fulfilling its obligations under this legislation.

The company needs to keep personal information secure, but it goes much wider than appropriate security and requires a comprehensive approach to the collection, use, sharing and retention of personal information, in order to build public/staff/client confidence. Combined with the reliance on fast changing ICT capabilities and storage of vast amounts of data, it is essential that Godfrey Group has this overarching document in plain language, which makes clear, to the public, the staff and the clients, the company's approach to data protection and data sharing; and explains the rights of the individual in relation to the information we hold about them. Publishing a clear and explicit policy and having the right approach to raising awareness and skills of staff, as they handle personal information, will be regarded as an integral element in promoting trust in the way this company handles the personal data entrusted to it.

The Data Protection Act 2018 controls how personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race

- ethnic background
- political opinions
- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

We have all been made aware of high profile data breaches, and many will be will be aware of the Information Commissioner's powers to fine up to 10 million euros, or 2% of a company's worldwide revenue, for severe breaches. Many of the reported breaches are however simply down to human error, such as inputting the incorrect fax number, emailing the wrong recipient or not checking personal data before it is posted, leaving sensitive documents in the car or not checking a person's identity over the phone. These errors can all be avoided by our directors, office staff and managers taking extra care in going about their duties and treating others' personal information, as they would their own. The company's leadership team have an important role to play in proper oversight of it's systems and processes so it makes breaches less likely.

In addition, in respect of any data processing generally, I am pleased to sign off a 'Personal Information Promise' - it is a form of mission statement for the handling of personal information aimed at those whose personal information we hold. If a compliance problem occurs we will reflect on whether we are living up to this promise, and I urge all staff to read this promise as it puts the Data Protection Act 2018 obligations into straightforward language that we can all understand and put into practice.

PERSONAL INFORMATION PROMISE

We, Andrew Godfrey and Louisa Godfrey, Directors of Godfrey Group Facilities Ltd, promise that we will:

1. Value the personal information entrusted to us and make sure we respect that trust;

2. Go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;

3. Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;

4. Be fair, open and transparent with individuals about how we use their information and who we give it to;

5. Make it easy for individuals to access, correct and request erasure (where we have no reason to retain), of their personal information;

6. Keep personal information to the minimum necessary and delete it when we no longer need it;

7. Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;

8. Provide training to staff who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;

9. Put appropriate resources into looking after personal information to make sure we can live up to our promises; and

10. Regularly check that we are living up to our promises and report to the external regulators on how we are doing.

Signed: Andrew Godfrey, Louisa Godfrey
Dated reviewed: 30.01.25

Introduction
Godfrey Group shall <u>at all times</u> comply with its duties under the Data Protection Act 2018 and the rights of privacy and respect for personal and family life set out in Article 8 of the Human Rights Act 1998.

The Data Protection Act 2018 (the Act) places legal obligations on organisations who collect and use personal information and gives individuals certain rights. In addition, there are stricter requirements in the Act in respect of processing 'special category data'. Personal information can be held in any format eg electronic, paper records, CCTV or photographic images and the Act applies, irrespective of how the information is held.

Responsibility for the Act
Godfrey Group is committed to ensuring all staff and contractors comply with the Act. The Company has an appointed a Data Protection Officer who is responsible for ensuring compliance with the Act.

There is a separate policy in respect of the Freedom of Information Act. Where a request is received under the FOIA or the EIRs but in fact it falls within the Data Protection regime, the company will automatically channel it through the appropriate policy, as it is required to do, as different exemptions and therefore, different legal rights apply in the circumstances.

Scope

This policy applies to all personal information held in any recorded format such as email, paper, video, CCTV or photographic images and applies to all staff who process personal data on behalf of the company. It is a criminal offence to destroy personal information when the purpose of the destruction was to avoid disclosure following a request.

Adhering to the 6 principles of the Act

The Data Protection regime is underpinned by 6 certain fundamental principles, which form a code for the proper processing of personal data. Processing means anything we do with data; such as obtaining, copying, disclosing, altering, retaining or destroying information. If we cannot comply with all these 6 principles, we should not be processing the data. The principles are summarised in the following diagram:

6 DATA PROTECTION PRINCIPLES

1. Personal data must be lawfully, fairly and transparently processed

2. Personal Data shall be collected for specified, explicit and legitimate purposes

3. Personal data shall be adequate, relevant and limited to what is necessary

4. Personal data must be accurate and up to date

5. Personal Data shall be kept in a form which permits identification for no longer than necessary

6. Personal data shall be held ensuring appropriate security

Data Protection applies to information kept on staff, customers and account holders, for example when we:

- recruit staff
- manage staff records
- market our products or services
- use CCTV

This could include:

- keeping customers' addresses on file
- recording staff working hours
- giving delivery information to a delivery company

In meeting our GDPR obligations Godfrey Group will ensure that: -

- It has in place procedures for complying with the six principles.

- Training on our data protection duties shall be mandatory for all staff. All new staff receive appropriate data protection training on induction and that refresher training and guidance is provided periodically, so that they understand that they are contractually responsible for complying with the law and know how to process information in accordance with these 6 principles.

- Advanced level training is provided to those members of staff who deal with highly sensitive personal information, where this may be required or relevant.

- Everyone managing and handling personal information are individually and collectively responsible for compliance with this policy.

- A failure to follow this policy may result in disciplinary action or even criminal prosecution in the case of a wilful and deliberate breach.

- That individuals are informed of the purposes for which their data will be used and that consent is sought for such use, where required under the Act. Examples of model privacy notices are attached as an appendix to this policy.

- All staff are trained to recognise a subject access request and what to do about one.

- All appropriate, technical and organisational security measures to safeguard personal information will be put in place including encrypting or ensuring

increased security settings of removable devices such as laptops or mobile phones and restricting the use of USB sticks.

- All staff are required to report data security breach incidents, including 'near misses' to their line manager who shall inform the Directors immediately.

Individual's Rights

The company will ensure that individuals can exercise their rights as set out in the Act including:-

- the right to be informed of the purposes of the processing;
- the categories of personal data being processed;
- the right of subject access to their personal information;
- who will or is likely to receive their information;
- the envisaged period for which the data will be stored;
- the right to prevent processing of personal information in certain circumstances;
- the right to rectify, block, erase, restrict, object or correct inaccurate information;
- the right to lodge a complaint;

These rights apply to all living, identifiable individuals on whom the company processes personal information.

Subject Access Requests

Article 15 of the GDPR provides the right for individuals to be told by the Data Controller (the organisation who determines the purposes for which and the manner in which personal information is processed)

- if we hold information about them,
- to ask what we use it for,
- to be given a copy of the information,
- to be given details of other organisations or people we disclose it to,
- to ask for incorrect data to be corrected,
- to ask us not to use personal information about them for direct marketing,
- to be compensated for damage or distress if we do not comply with the Act,

- to object to decisions made only by automatic means – for example where there is no human involvement,
- to ask the Information Commissioner's Office to investigate and assess whether we have breached the Act.

The company will supply this information providing the request is made verbally or in writing, and it is sufficiently clear what personal information is being sought; therefore sufficient information should be given by the applicant to enable the company to locate the information requested.

There is no fee applicable and the company should respond within one month, unless the request is complex or multiple, in which case it may be extended by two further months. The company will inform the applicant if it is extending the time frame in such circumstances setting out the reasons as to why.

The company will respond to such requests within one month, unless the request is manifestly unfounded or excessive. There is no definition within the Act, but in respect of an 'excessive' request, it is generally taken to mean that the effort the organisation would have to expend in complying with the requirement to provide a copy, is disproportionate to the benefit to be derived by the individual in receiving it. In such circumstances the company will refuse the request.

Advice should be sought from the company's Data Protection Officer in the first instance, ideally before the company commence their search and collation of the data.

Where the individual makes a request electronically, the company will provide the information in a 'commonly used electronic format' in accordance with the GDPR; unless the applicant requests otherwise.

A request for personal information should be submitted on the standard form in

<u>What if the data includes information about other people?</u>
Applicants will not automatically be given access to parts of their information which also identify other people, without that third party's agreement, even if they are related. Disclosure will depend on the context and whether information is already within knowledge and all the circumstances of the case. Seek advice if in doubt.

The Act says that the company would not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information, the company must take into account all of the relevant circumstances, including:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the other individual;
- any steps taken to seek consent from the individual;
- whether the other individual is capable of giving consent;
- any express refusal of consent by the individual.

These are areas should be taken into account, but they are not necessarily determinative, as the decision is one for the company to make, balancing the data subject's rights against other individual rights.

Requests from third parties (eg the Police) for an individual's personal information

Occasionally the company may receive formal requests under the Act from other agencies or third parties such as the police, DWP or HMRC, solicitor's firms etc, to physically access or receive a copy of the information relating to an individual. These sections do not provide the company with an automatic reason to disclose, as is explained below.

The Act deals with several situations in which personal data is processed for the following 'crime and taxation' purposes:

- the prevention or detection of crime;
- the capture or prosecution of offenders; and
- the assessment or collection of tax or duty.

The personal data could be disclosed if the disclosure is for any of the above crime or taxation purposes and the above purposes are 'likely to be prejudiced' if the company did not disclose eg to the police or the inland revenue. The threshold for disclosure in these circumstances needs to be more than a mere risk of prejudice and needs to be a significant and weighty chance of prejudice to the above purposes. In such circumstances you would need the third party to set out what information they wanted to see (or envisaged) and what legal powers they are relying on and evidence of identity. Seek advice from the Data Protection Officer or legal services if in doubt.

Disclosure of personal information over the telephone or face to face without establishing the identity of the recipient should be avoided.

What about our external suppliers and the company outsourcing personal data processing?

The company uses third party organisations to perform some of it's functions. Where such 'outsourcing' arrangements involve the processing of personal data,

certain legal obligations are placed on the company to ensure this supplier looks after the personal information in the same secure way as the company does. These obligations are more onerous now under GDPR than under the old data protection legislation therefore extra care needs to be taken when entrusting a third party supplier with personal data. Seek advice if you are in doubt.

Introduction of new systems that affect personal information – what should the company consider?

In developing information systems or new business processes or changes to our existing processes, that involve personal information, it is now a requirement to carry out a Data Protection Impact Assessment (DPIA) and to build in privacy-friendly solutions as part of modernising or introducing new systems. This is referred to under the GDPR as 'Privacy by Design and Default' and the DPIA can be a useful tool to help identify risks and help the School manage those risks and where possible eliminate them.

Email use

Company staff should only use an authorised email account to communicate in respect of Godfrey Group business and functions. Under no circumstances should staff (including fixed term, temporary, supply, agency or otherwise) use their personal email account to communicate with regards to company issues, in order to protect all individuals concerned. Any staff member communicating in breach of this policy may face disciplinary action.

Data Security Breaches

All data security breaches, including 'near misses', must be reported to the Line Manager responsible, who shall immediately inform the Director who shall advise on the necessary steps that need to be taken to contain any resultant damage and inform individuals who may be affected. A central record of all breaches will be retained and serious breaches must now be reported to the Information Commissioner's Office. There is a standard breach notification form on their website.

Oversight arrangements and review of policy

This policy will be reviewed no later than December 2024. Compliance with this policy and related procedures will be monitored by the Directors.

Complaints

A review of the company's decision to *withhold* personal information where an applicant has made a subject access request, can be made to the Company's Data

Protection Officer who will facilitate a review. If the decision is upheld, and the applicant remains unsatisfied they may appeal to the Information Commissioner's Office

Contact details

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel 01625 545745
www.informationcommissioner.gov.uk

Appendix 1
Seven golden rules
for information sharing

1. **Remember that the Data Protection Act is not a barrier to sharing information** but provides a framework to ensure that personal information about living persons is shared appropriately

2. **Be open and honest** with the person (and/or their family where appropriate) from the outset about 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.

3. **Seek advice** if you are in any doubt, without disclosing the identity of the person where possible.

4. **Share with consent where appropriate** and, 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.

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:** 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.

7. **Keep a record** of your decision and the reasons for it – 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.