ESH GROUP
DATA PROTECTION POLICY

Policy Author:	Mark Sowerby, Group Chief Financial Officer
Date:	April 2018
Policy Review Date:	2019
Policy Owner:	Mark Sowerby, Group Chief Financial Officer

1 Policy Statement

Esh Group needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

This data protection policy ensures Esh Group:

- Complies with data protection law and follow good practice;
- Protects the rights of staff, customers and partners;
- Is open about how it stores and processes individuals' data; and,
- Protects itself from the risks of a data breach.

The General Data Protection Regulation (GDPR) which replaces the Data Protection Act 1998 (DPA) in May 2018, describes how organisations — including Esh Group and all its subsidiary companies — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR and DPA are underpinned by eight key principles. These say that personal data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Processed in accordance with the rights of data subjects;
7. Be protected in appropriate ways; and,
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Failure to comply with GDPR can result in the Company being subject to audit by the Information Commissioner's Office and potentially large fines.

2 Scope

This policy applies to all employees, sub-contractors, agency workers, volunteers, partners and suppliers working for or on behalf of Esh Group, otherwise referred to as workers.

It applies to all data that the Group holds relating to identifiable individuals. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- Photographs; and,
- Any other information relating to individuals.

This policy helps to protect Esh Group and individuals from some very real data security risks, including the following.

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

3 Policy

3.1 Responsibilities

3.1.1 Everyone who works for, or with Esh Group has some responsibility for ensuring data is collected, stored and handled appropriately.

3.1.2 Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

3.1.3 The Board of Directors is ultimately responsible for ensuring that Esh Group meets its legal obligations.

3.1.4 Esh Group recognises the need, under GDPR, for a board member to hold the overall accountability for data protection. The designated Data Protection Officer at Esh Group is Mark Sowerby, Group CFO, who is accountable for:

- Keeping the board updated about data protection responsibilities, risks and issues;
- Ensuring all data protection procedures and related policies are reviewed, in line with an agreed schedule;
- Ensuring ongoing data protection training and advice is in place for the people covered by this policy;

- Arbitrating data protection questions from staff and anyone else covered by this policy where line management and data controllers have been unable to reach a conclusion;
- Ensuring requests from individuals to see the data held by Esh Group (also called 'subject access requests') are processed in accordance with the DPA/GDPR; and,
- Ensuring robust checking and approval of any contracts or agreements with third parties that may handle the company's sensitive data.

3.1.5 The Head of IT is accountable for:

- Ensuring all systems, services and equipment used for storing electronic data meet acceptable security standards as documented in the IT Security Policy;
- Ensuring regular checks and scans take place to provide reassurance that security hardware and software is functioning properly; and,
- Ensuring that any third-party services the company is considering using to store or process data are adequately evaluated. For instance, cloud computing services.

3.1.6 The Business Development Director is responsible for:

- Approving any data protection statements attached to communications such as emails and letters;
- Addressing any data protection queries from journalists or media outlets like newspapers; and,
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

3.1.7 A Data Controller is an individual whose job responsibilities require them to determine the purpose and means of processing personal data. This will usually be the Business Director.

3.1.8 The Data Subject is an individual who is the subject of personal data. In other words, the Data Subject is the individual whom particular personal data is about.

3.2 Data Storage

3.2.1 These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to line management, data controllers or the Data Protection Officer.

3.2.2 When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

3.2.3 These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Workers should make sure paper and printouts are not left where unauthorised people could see them, such as on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

3.2.4 When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Personal and sensitive data held in documents outside of the core Esh business systems (e.g. Oracle, Sage, Viewpoint), should be protected by strong passwords (compliant with the requirements of the IT Security Policy) that are changed regularly and never shared between individuals.
- If data is stored on removable media, such as USB sticks (compliant with the requirements of the IT Security Policy), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures (see IT Security Policy).
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall (see IT Security Policy).

3.3 Data Use

3.3.1 Personal data is of no value to Esh Group unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft. Accordingly:

- When working with personal data, workers should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be distributed by email unless encrypted as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. IT Services can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Workers should not save copies of personal data to their own computers. Always access and update the central copy of any data.

3.4 Data Accuracy

3.4.1 The law requires Esh Group to take reasonable steps to ensure data is kept accurate and up to date.

3.4.2 The more important it is that the personal data is accurate, the greater the effort Esh Group should put into ensuring its accuracy.

3.4.3 It is the responsibility of all workers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Workers should not create any unnecessary additional data sets.
- Workers should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

- Esh Group will make it easy for data subjects to update the information Esh Group holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

3.5 Subject Access Requests

3.5.1 All individuals who are the subject of personal data held by Esh Group are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.
- Request that the data is deleted, unless this would contradict a legal or regulatory requirement.

3.5.2 If an individual contacts Esh Group requesting this information, this is called a subject access request.

3.5.3 Subject access requests from individuals should be made by email, addressed to the Data Controller. The Data Controller can supply a standard request form, although individuals do not have to use this.

3.5.4 Individuals will not be charged for reasonable subject access requests. The data controller will aim to provide the relevant data within 14 days. Where they are unable to provide this information in the time period or when they believe the request is unreasonable, they should consult with the Data Protection Officer.

3.5.5 The data controller will always verify the identity of anyone making a subject access request before handing over any information.

3.5.6 For detailed information refer to the procedure 'Dealing with Subject Access Requests'.

3.6 Disclosing Data for Other Reasons

3.6.1 In certain circumstances, the GDPR and the DPA allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

3.6.2 Under these circumstances, Esh Group will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

3.7 Providing Information

3.7.1 Esh Group aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used; and,
- How to exercise their rights.

3.7.2 To these ends, the company will issue a privacy statement, setting out how data relating to individuals is used by the company.

3.8 Reporting a Breach

3.8.1 In the event of a breach, refer to the document 'Process for reporting a Personal Data Breach' for detailed information on the steps to take.

4 Policy Compliance

4.1 Compliance Measurement

4.1.1 Internal Controls and the Audit team proactively monitor activities to ensure compliance with this policy and the GDPR.

4.2 Exceptions

4.2.1 Any exception to the policy must be endorsed by the appropriate Business Director (Data Controller) and the Data Protection Officer.

4.3 Non-Compliance

4.3.1 An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5 Further Information

If an employee feels that their role requires them to handle a high level of Personal Data and they believe their knowledge requires improvement, then they should raise with their line manager or the Data Protection Officer and appropriate training will be provided.