DATA RESPONSE PROTOCOLS

The following document gives details of our response protocols in the case of :

1) **Data Subject access request**

2) **Data Subject rectification and erasure requests**

3) **Data Breach**

1. Data Subject Access Requests

1.1 Data subjects whose personal information we process have a legal right to request access to the personal data we hold about them.

1.2 There may be occasions where we have a legal right to refuse that access but these occasions will not be the norm. A refusal to disclose information is a decision that must only be taken after consultation with the Privacy Officer.

1.3 Any Data Access request must be notified immediately to the Privacy Officer.

1.4 The Privacy Officer is entitled to require the requester to verify their identity and put their request in writing, particularly if she / he has any concerns about the identity of the requester or the validity of the request.

1.5 Data Access requests must be responded to fully within 30 days. The Privacy Officer should initially acknowledge the request in writing (or by email if the request was received by email).

1.6 All Staff are required to promptly respond to any request from the Privacy Officer for information about personal data held by our station and how it has been processed, for the purposes of making a response to a Data Access request. All Staff must promptly provide copies of that personal data to the Privacy Officer in the format requested by the Privacy Officer when requested to do so. The importance of a complete and full disclosure of all personal data we hold about the data subject cannot be overstated.

1.7 Reception staff and other Staff members who receive telephone, email or in person requests for disclosures of any personal data from individual data subjects should ask the data subject to send an email or put their request in writing. You can tell the requester that their written / email request and that it will be passed on immediately to the person in our organisation who handles Data Access requests.

1.8 A sample Data Access Disclosure Letter is attached at Appendix A to this Policy.

2. Data Subject rectification and erasure requests

2.1 A request for rectification or erasure of personal data we hold about a data subject will usually be made following release to the data subject of their personal data held by us pursuant to a Data Access request.

2.2 We will promptly rectify (by way of updating, correcting any inaccuracy in or addressing a deficiency in the personal data we hold about that person) and confirm to them in writing (or by email) that we have done so.

2.3 We will promptly erase any personal data we hold about a data subject where that person has requested the erasure of that personal data *unless we believe we are entitled to keep that data;*

2.3.1 for exercising our right of freedom of expression and information;

2.3.2 for the performance of a task in the public interest;

2.3.3 for archiving purposes in the public interest;

2.3.4 for the purposes of legal claims to which our station or any of our station personnel are a party.

2.4 The exemptions set out at clauses 2.3.1 and 2.3.3 above are likely to be relevant if our news or programme archive contains content that a data subject wishes to have erased. In these instances, the data subject should be requested to put their request in writing and the Department / Output Area manager and the Privacy Officer will discuss and decide on the appropriate response to the request.

2.5 All rectification and erasure requests must be notified to the Privacy Officer and the Privacy Officer shall keep a record of all rectification and erasure requests received and the actions taken following such requests.

1. Data Breach

There are two people to whom we must report data breaches – unless reporting is not necessary as indicated below.

- The Data Protection Commissioner
- The data subject whose personal data we have lost or otherwise compromised.

Reporting internally

1.1 A data breach occurs when personal data held by Learning Waves is inadvertently lost, stolen or otherwise disclosed or at risk of disclosure to a third-party to whom we are not authorised to disclose that data, or the security and integrity of the personal data we hold is otherwise compromised.

1.2 Learning Waves has serious legal obligations and liabilities in the event of a data breach. We are at risk of being fined by the Data Protection Commissioner and / or sued for damages by the data subjects concerned.

1.3 Where our data security systems fail for any reason and data is disclosed or its security or integrity compromised, even accidentally, that data breach *must* be reported immediately to the Privacy Officer, with a full report of the what data has been lost / disclosed and how the breach occurred.

1.4 Immediate action must be taken, in liaison with the Privacy Officer, to limit any harm or damage to the data subjects concerned and limit, if possible, the risk of unauthorised access to the data.

Reporting externally

1.5 The Privacy Officer in liaison with the relevant person/manager will immediately assess whether the breach is likely or unlikely to result in a risk to the rights and freedoms of the data subject affected.

1.6 The Privacy Officer must report the breach in writing to the Data Protection Commissioner in writing within 72 hours of becoming aware of the breach

unless she / he concludes that the breach is *unlikely to result in risk* to the rights and freedoms of the data subjects affected.

1.7 The report to the Data Protection Commissioner should include the following information:

1.7.1 nature of the breach;

1.7.2 categories and approximate number of data subjects concerned;

1.7.3 categories and approximate number of personal data records concerned;

1.7.4 name and contact details of Privacy Officer who can supply more information if required;

1.7.5 likely consequences of the breach;

1.7.6 measures taken by us to address and mitigate the adverse consequences of the breach.

1.8 Whether liable to be reported or not, the Privacy Officer will keep records of all data breaches so that the information is available for production to the Data Protection Commissioner in the event of an investigation or audit by her / his Office of our compliance with our breach reporting obligations.

1.9 Note that we encrypt our laptops and implement equivalent security measures in respect of our other digital devices because *encryption and equivalent security measures mean the breach is unlikely to result in risk* to the rights and freedoms of the data subject affected and reporting to the Data Protection Commissioner will not be necessary.

Reporting to the data subject(s) affected by a data breach

1.10 The Privacy Officer in liaison with the relevant person/manager manager will immediately assess whether the breach is likely or unlikely to result in a *high risk* to the rights and freedoms of the data subjects affected.

1.11 We are legally obliged to report a data breach to the data subject affected *if* the breach is likely to result in *high risk* to the data subject affected. Where the Privacy Officer concludes that such high risk exists, then a written communication of the breach must be sent to the data subject without undue delay.

1.12 Where the Privacy Officer communicates the data breach to the data subject affected, she / he shall ensure that the communication states:

1.12.1 the nature of the data lost / in respect of which the breach has occurred;

1.12.2 the name and contact details of the Privacy Officer and that more information can be obtained if required from the Privacy Officer;

1.12.3 describe the likely consequences of the breach;

1.12.4 describe the measures taken or to be taken by our station in respect of the breach (e.g. reporting to Data Protection Commissioner) and any steps we will take to mitigate the adverse consequences of the breach.

1.13 Note that we encrypt our laptops and implement equivalent security measures in respect of our other digital devices because *encryption and equivalent security measures mean the breach will not result in a high risk* to the rights and freedoms of the data subject affected and communication of the breach to a data subject will not be necessary.