APPENDIX C

GDPR – SECURITY INCIDENT/DATA LOSS MANAGEMENT PROTOCOL

In order to comply with the requirements of the GDPR we are required to record and investigate any security incident or data loss.

WHAT IS A SECURITY INCIDENT?

An information security incident can occur when the confidentiality, availability and or integrity of the Learn to Live Federation's information is put at risk.

Examples of activities considered an information security incident might include:

- Information being at risk of or being lost; stolen; disclosed to the wrong recipients (accidentally or deliberately); accessed or attempted to be accessed unlawfully and/or without the permission of the Learn to Live Federation; sold or used without the permission of the Learn to Live Federation or a system containing personal data or sensitive business data malfunctions and the information is irretrievable indefinitely or for a long period of time.

Other examples of information security incidents might include:

- losing paper files or documents containing personal or sensitive business data;
- faxing or emailing personal or sensitive business data to the wrong recipients;
- posting personal or sensitive business data to the wrong recipients;
- deliberately or accidentally disclosing personal or sensitive business data to people who are not legally entitled to the information;
- using or selling personal or sensitive business data without the permission of the Learn to Live Federation;
- deliberately or accidentally sharing a password or entry code to an office, computer system or files containing personal or sensitive business data, to someone who is not ordinarily entitled to see the information;
- computer equipment containing personal or sensitive business data is lost or stolen;
- a business critical system containing personal or sensitive business data malfunctions and the information cannot be retrieved quickly;
- computer viruses, malware attacks or phishing scams against the IT systems;
- unauthorised access or attempted access to IT systems or secure areas.

WHEN TO REPORT

Any security incident, suspected security incident or near miss should be reported to the Data Protection Officer, Dave O'Loughlin, as soon as possible. In the absence of the Data Protection Officer being available, the incident should be reported to any member of the Senior Leadership Team.

Do not delay reporting an incident whilst you look for the lost information, report the loss as soon as it is identified.

HOW TO REPORT

If the incident relates to pupil or parent information it can be reported via CPOM's using the Data Loss category. If the incident relates to staff data or multiple pupils it should be logged within CPOMs, Data Loss category against "No Pupil".

LOGGING A SECURITY INCIDENT

The Data Protection Officer is responsible for overseeing information security incidents, upon being notified of an incident the following steps will be taken:

- The incident will be logged in the Learnt to Live Federation's incident log – kept on the CPOMs system;
- The Data Protection Officer will acknowledge receipt of the incident within two working days;
- Sufficient evidence to enable a risk assessment or privacy impact assessment to be gathered within two working days;
- An assessment of the severity of the incident to be carried out within three working days;
- Notify the Executive Head and relevant Governor if the incident will require reporting to the Information Commissioner's Office or if other appropriate action needs to be taken.

Every incident will be categorised according to the nature of the incident, the sensitivity of the data involved and the number of data subjects affected. If this is not immediately apparent it will be established during the investigation.

If a particular individual or team are repeatedly causing the same type of incident this will be referred to the Executive Head and HR Department for further advice and possible disciplinary action.

INCIDENT CLASSIFICATION AND NOTIFICATION

Incidents will be classified as follows:

Incident Classification	Description	Notification
No Incident	The incident has not jeopardised the confidentiality, availability or integrity of data.	Line manager of the person reporting and any other involved staff.
No Incident – Near Miss	There is a risk that the incident might adversely affect the confidentiality, availability or integrity of data but this has not materialised in this case.	Line manager of the person reporting and any other involved staff.
Low Risk Incident	The confidentiality, availability or integrity of data has been adversely affected however the impact on the Learn to Live Federation and any data subjects involved is negligible.	Line manager of the person reporting and any other involved staff.
Medium Risk Incident	The confidentiality, availability or integrity of data has been significantly affected and there is a measurable impact on the Learn to Live Federation. The incident has not impacted adversely on the rights and freedoms of the data subject.	Line manager of the person reporting and any other involved staff, Executive Head and HR Manager.
High Risk Incident	The confidentiality, availability or integrity of data has been impacted to such an extent that there are significant business continuity risks. The incident has caused a negative effect on the rights and freedoms of the data subject.	Executive Head and relevant Governor.

NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE (ICO)

The ICO will be notified within 72 hours of any incident which might adversely affect the rights and freedoms of a data subject. The ICO interactive reporting tool will be used as part of this assessment.

Notification is the responsibility of the Data Protection Officer following consultation with the Executive Head.

INFORMATION SECURITY INCIDENT INVESTIGATION

The Data Protection Officer will complete an information security investigation and notify relevant staff of the outcome within twenty days of the incident being notified.

Key points are:

- The notification will include a summary of the incident, lessons learnt, action points and relevant guidance.
- If personal data has been inappropriately disclosed, action will be taken to retrieve the data.
- If a member of staff has been negligent, malicious or unreasonable then the HR Manager will decide if further investigation or action is necessary.
- If staff member's actions may constitute an offence under GDPR or the Computer Misuse Act 1990, the matter will be reported to Devon & Cornwall Police.

NOTIFYING DATA SUBJECTS

All incidents which may have a negative impact on the rights and freedoms of data subjects will be notified without undue delay. The notification will include:

- An apology.
- A description of the information put at risk.
- A description of any risk this may cause the data subject.
- A description of how the incident occurred.
- Details of steps taken to remedy the incident and prevent reoccurrence.
- Guidance on how to protect themselves from the effect of the incident.
- Details of how to make a formal complaint to the Learn to Live Federation and the ICO.
- Details of who has been informed of the incident.

The notification will be made in writing.

REVIEW OF INCIDENTS

The Data Protection Officer will ensure that incidents are recorded, monitored and escalated as appropriate.

Actions proposed in response to an incident will be monitored by the Data Protection Officer and reported to Governors on a termly basis.

If actions are not completed or if similar incidents continue, the Data Protection Officer will inform the Executive Head and HR Manager.

RECORD KEEPING

Records of security incidents, investigations and actions will be kept via the CPOMs system.

APPENDIX C TO BE READ IN CONJUNCTION WITH THE DATA PROTECTION POLICY