Handling School Data Policy

All Tucasi Limited employees, contractors and partners are required to read, understand and adhere to the following Tucasi company policy regarding the use and storage of school data held within Tucasi.

Throughout this document, 'school data' relates to any SCO databases, pupil or staff data import files and any log files that contain personal data. 'School' refers to any educational establishment.

Handling School Data

All Tucasi employees should be aware of The Data Protection Act 1998 – see Appendix 1.

1. School data should only be handled when absolutely necessary, and then only by Tucasi employees in the Customer Support Team or Development Team or other staff that provide assistance to Customer Support Team or Development Team as required.
2. All other Tucasi staff, contractors, partners should not handle or use pupil or staff data provided to Tucasi by schools without express permission from the Managing Director of Tucasi.
3. For product demonstration and training purposes, Tucasi will provide a demonstration/ training database containing fictitious pupil and staff data.
4. During the course of training a school the Tucasi training team may have sight of, and help to import, school data into a school system. At no time should Tucasi trainers take a copy of the school data. If data needs to be sent to Tucasi it should be emailed to the Tucasi Customer Support Team direct from the school or transferred by secure FTP using one of the Tucasi FTP accounts.

School Data Protection

5. All schools databases are protected by unique passwords to prevent unauthorised access.
6. School data available to Tucasi employees must be treated as strictly confidential. Details of pupil, or staff, data should not be disclosed to anyone outside of the company.
7. All Tucasi employees will be required to undergo a Criminal Records Bureau check which will be paid for by Tucasi. See http://www.crb.homeoffice.gov.uk/ for further information on CRB checks.

Storing School Data

8. All school data should be saved and stored only on the Tucasi office server.
9. Under no circumstances can school databases, or any pupil-related data in the form of emails, attachments or other, be held on laptop computers, or other portable device (memory sticks, CD, etc) that are removed from the office.
10. Databases may be temporarily transferred onto local computers only as far as is needed for the purposes of investigating or fixing the school database. The local computers should ideally not be laptops and if laptops are used they cannot be removed from the Tucasi office whilst school data remains loaded on the computer. After the database has been investigated, fixed or repaired, the copy must be returned to the server. Databases should be copied directly from the server to the relevant client machine, and not transferred by email or Skype.
11. School data should NOT be saved onto local computers any longer than is absolutely required for the purposes of investigating or fixing school databases.

Data Transfer

12. School data that requires investigation by Tucasi should be sent via email direct to support@tucasi.com or transferred by secure FTP using one of the Tucasi FTP accounts.
13. School data should NOT be sent to personal or individual email addresses within or outside of Tucasi.
14. Emailed data should be saved onto the Tucasi office server by the Customer Support Team member monitoring emails, and the recipient alerted accordingly.
15. Databases that have been repaired and require to be returned to schools should only be sent to email addresses authorised by the school.

Deletion of School Data

16. Any local copy of data must be deleted after use.
17. Attachments should be deleted from Microsoft Outlook or other email programs.
18. Data should be deleted from the Recycle Bin.
19. Unless the school has given prior permission, databases held for more than 1 year will be deleted from the Tucasi office server. A member of the Customer Support Team will review and delete databases older than one year from the server on an annual basis during the summer holiday period.

Breach of Guidelines

20. Any breaches of this policy will be deemed as serious breach of trust and could lead to disciplinary action. Depending upon the severity of the breach this could include dismissal without notice.

Policy Drafted	Karen Murtagh	11 August 2010
Policy Approved	Peter Redding	11 August 2014
Date for review		11 August 2016

Appendix 1

The Data Protection Act 1998

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Should an individual or organisation feel they're being denied access to personal information they're entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office for help. Complaints are usually dealt with informally, but if this isn't possible, enforcement action can be taken.