ST ALOYSIUS' COLLEGE

DATA PROTECTION POLICY

1. Introduction

In common with all educational establishments, the St Aloysius' College holds and processes information about its employees, applicants, past and present parents, pupils, and other individuals for various purposes (for example the administration of the admissions process, the effective provision of academic and welfare services, to record academic progress, to operate the payroll and to enable correspondence and communications, including the provision of references and certificates). To comply with the Data Protection Act 1998 (the 1998 Act), information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. Top Tips from the Information Commissioner on how to protect personal data held are to be found at Appendix One.

Definitions for "personal data" and "Data Controller" can be found in Appendix Two.

2. Notifications to the Information Commissioner

The St Aloysius' College has an obligation, as a Data Controller, to notify the Information Commissioner of the purposes for which it processes personal data. Individual data subjects can obtain full details of the St Aloysius' College's data protection registration with the Information Commissioner from the School Data Protection Officer (the Data Protection Officer) or from the Information Commissioner's website (www.ico.gov.uk).

3. Data Protection Principles

The St Aloysius' College, as a Data Controller, must comply with the Data Protection Principles, which are set out in the 1998 Act. In summary the Data Protection Principles state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions (which can be found in Schedules 2 and 3 of the 1998 Act) are met
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes
- Be adequate, relevant and not excessive for those purposes
- Be accurate and kept up to date
- Not be kept for longer than is necessary for the purposes it is being processed
- Be processed in accordance with the data subject's rights under the 1998 Act
- Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss, damage or destruction
- Not be transferred to a country or territory outside the European Economic Area, unless that country or territory has adequate levels of protection for the rights and freedoms of data subjects in relation to the processing of personal data

4. Processing

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) Organisation, adaptation or alteration of the information or data,
(b) Retrieval, consultation or use of the information or data,
(c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) Alignment, combination, blocking, erasure or destruction of the information or data.

5. Data Protection Officer

The St Aloysius' College Data Protection Officer is the Data Protection Officer. All queries about The St Aloysius' College policy and all requests for access to personal data should be addressed in the first instance, to the Data Protection Officer, James Cluckie. (see "Rights to Access Personal Data" below).

6. Responsibilities of Individual Data Users

All St Aloysius' College staff who record and/or process personal data in any form must ensure that they comply with the requirements of the 1998 Act (including the Data Protection Principles) and with the St Aloysius' College Data Protection Policy (including any procedures and guidelines which may be issued from time to time). A breach of the 1998 Act and/or the St Aloysius' College Data Protection Policy may result in disciplinary proceedings.

In particular, no member of staff may, without the prior written authorisation of the Data Protection Officer:

- Develop a new computer system for processing personal data
- Use an existing computer system to process personal data for a new purpose
- Create a new manual filing system containing personal data
- Use an existing manual filing system containing personal data for new purposes

The above does not apply to databases which are maintained by staff within the St Aloysius' College for their private domestic use, for example, private address books.

7. Data Security and Disclosures

All members of staff are responsible for ensuring that:

- Any personal data which they hold is kept securely

- Personal data is not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to ensure that data is not disclosed accidentally

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct. If in any doubt, staff should consult the St Aloysius' College Data Protection Officer.

Personal data must be kept securely and examples of how this may be done will include:

- Keeping the data locked in a filing cabinet, drawer or room, or otherwise inaccessible to unauthorised persons;

- If the data is electronically stored on computer or other electronic device, ensuring that the data is password protected or kept only on disk which is itself kept securely; or
- Any other reasonable and appropriate security measure.

8. Data Handling

Personal data should be handled and access to it permitted on a strictly "need to know" basis.

Any communications or documents containing personal data of a **sensitive or confidential** nature should carry an appropriate handling caveat. In practical terms, this means applying a "CONFIDENTIAL" header and footer to the communication or document, whether it is being electronically stored, handled or transmitted, or manually so (i.e. by hard copy, on or separate from a manual file). It is extremely important that handling caveats are used scrupulously and fully respected by data users. Password protection on individual electronic documents should be used in appropriate circumstances, such as when transferring documents containing sensitive information.

All documents or files being moved manually from one person or department to another within the St Aloysius' College must be placed in a sealed envelope, which must be clearly and specifically addressed to a named individual. This applies both to files and to individual documents and the envelopes must be clearly marked with the handling caveat "CONFIDENTIAL. Personal for....."

9. Obligation to provide and maintain accurate and up-to-date Personal data

All staff must endeavour to ensure that any necessary personal data provided to the schools, on themselves or any third party is accurate and up-to-date. Staff are responsible for providing updates on changes to relevant personal data about them which is held by the School, e.g., changes of address, qualifications and the like.

Staff charged with responsibility for maintaining the School's structured filing systems (both electronic and manual) are to take all reasonable steps to ensure that personal data contained therein is kept accurate and up-to-date.

10. Data Subjects' Consent

It is a requirement of the 1998 Act that consent should be sought, whenever practicable, from individual data subjects for Data Controllers to hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The St Aloysius' College will consider any such objections, but reserves the right to process personal data in order to carry out its functions as permitted by law.

Consent can be sought on an "opt in" basis, where consent is specifically sought in writing, or an "opt out" basis whereby consent is assumed unless an individual elects to state that he or she withholds consent. It is self-evident that a school cannot undertake its functions in relation to pupils, parents, staff and former pupils without properly, reasonably and necessarily holding personal data about them. It is therefore, a reasonable conclusion that in enrolling a pupil, or accepting employment or otherwise freely becoming formally involved with the School, a parent, staff member or Director of the Court accepts this necessity and consents to personal data on them, (or their children, as pupils) being held and processed by the School. Any staff member who does not consent to personal data being held on them should advise the Data Protection Officer forthwith in writing.

11. Rights to Access Personal Data

Staff, parents, pupils of appropriate age under the law (in Scotland the law presumes that a child aged 12 years or more has capacity to make a request for access) and other individuals have the right under the 1998 Act to access any personal data that is being held about them either in an "automatically process-able form" (mainly computer records) or in a "relevant filing system" (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible, such as an individual's personnel file with an index and dividers separating information relating to personal details, holidays, sickness absence etc) and to request the correction of such data where they are incorrect. Any individual who wishes to exercise his or her right of access should do so in writing to the Data Protection Officer.

Any inaccuracies in data disclosed in this way should be communicated immediately to the Data Protection Officer who shall take appropriate steps to make the necessary amendments.

The St Aloysius' College reserves the right to make a charge of £10 (or such other charge as is permitted from time to time under the 1998 Act or any subsequent amendment to the 1998 Act) on each occasion that access is requested. In accordance with the 1998 Act, the St Aloysius' College reserves the right to refuse repeated requests where a reasonable period has not elapsed between requests. A reasonable period will be 60 days or any other time that the St Aloysius' College considers to be reasonable in the circumstances. In normal circumstances, the St Aloysius' College will not charge staff for access to personal data held on them.

It is the policy of the St Aloysius' College to be willing and open in its response to data access requests, respecting both the letter and the spirit of the law. The St Aloysius' College will normally respond to the request for access to personal data within 40 days (including bank holidays and weekends) of the request or payment of the fee, if payment is called for, whichever is the later. Requests for disclosure of pupil educational records must be complied with within 15 school days, in accordance with the Pupils' Educational Records (Scotland) Regulations 2003 (the 2003 Regulations"), at no charge. A charge may be applied in accordance with the 2003 Regulations where the request is for a copy of the information in its original format. This applies also to requests by past pupils.

12. Disclosure Outside of the European Economic Area (EEA)

The St Aloysius' College may, from time to time, require to transfer personal data to countries or territories outside of the EEA with the knowledge of, and for purposes made known to, individual data subjects. For example, the names of members of staff on a website may constitute a transfer of personal data worldwide. Accordingly, if an individual wishes to raise an objection to this disclosure then written notice should be given to the Data Protection Officer.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures are taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects. Exemptions for when personal data can be transferred to a country or territory outside the EEA, which does not ensure an adequate level of protection for the rights and freedoms of data subjects, can be found in Schedule 4 of the 1998 Act. A definition of "adequate level of protection" is set out in Appendix Two.

13. Sensitive Personal Data

The St Aloysius' College may from time to time process "sensitive personal data" relating to pupils, parents, candidates and staff of the St Aloysius' College.

"Sensitive personal data" is defined under the 1998 Act as information as to a data subject's racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, offences or alleged offences, and information relating to any proceedings for offences committed or allegedly committed by the data subject, including the outcome of those proceedings.

The St Aloysius' College needs to process some types of sensitive personal data. For example, data relating to the gender and ethnic origin of members of staff of the St Aloysius' College could be processed for the purposes of equal opportunities monitoring. Pupils' medical records need to be processed for the provision of health care and general welfare purposes. To comply with security vetting and/or Child Protection legislation the St Aloysius' College may need to process information regarding criminal convictions or alleged offences. Such processing will be undertaken only as and when strictly necessary and with absolute respect to individual confidentiality.

In certain circumstances, where sensitive personal data is to be held or processed, the St Aloysius' College may seek the explicit consent of the member of the St Aloysius' College Community in question unless one of the limited exemptions provided in the Data Protection Act 1998 applies (such as to perform a legal duty regarding employees or to protect the data subject's or a third party's vital interests).

14. CCTV

The St Aloysius' College operates a number of CCTV cameras in order to assist with security for members of the St Aloysius' College Community and in respect of the St Aloysius' College's property. Any staff wishing to raise any queries regarding the operation of the CCTV system should contact the Data Protection Officer. Anyone wishing to access any personal data about them on the CCTV system, should make a formal request to the Data Protection Officer with as much information as possible to enable the data to be located (including, if possible, details of the relevant camera, date and time). The St Aloysius' College operates a 30 day retention policy in respect of all CCTV footage. The St Aloysius' College reserves the right to levy a £10 fee for such requests.

15. E-mail

It is permissible and appropriate for the St Aloysius' College to keep records of internal communications which are relevant to an individual's on-going relationship with the schools, whether as a parent, member of staff or pupil, including information concerning performance and conduct issues, provided such records comply with the Data Protection principles.

It is recognised in law that e-mail is often used for such communications and that such e-mails should form part of the St Aloysius' College's records. It goes beyond the scope of this policy document to address the appropriate use of e-mail in the proper functioning of the school and the limitations and legal implications of this mode of communication. However, all members of the staff need to be aware that:

- The 1998 Act applies to e-mails which contain personal data about individuals which are sent or received by members of the St Aloysius' College Community (other than for their own private purposes as opposed to school purposes);

- Subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to e-mails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the St Aloysius' College to locate the personal data in the e-mails; and

- The legislation applies to all e-mails from and to members of the St Aloysius' College Community which are sent and received for St Aloysius' College purposes, whether or not the e-mails are sent through the schools' e-mail system or on an individual's own e-mail account however the use of personal email addresses for St Aloysius College business is not routinely permitted

16. Retention of Personal Data

The 1998 Act requires that personal data should be processed and retained for no longer than is necessary. Personal data should not be held indefinitely without reason, but there are legitimate business archive and historical archive purposes for which personal data may be retained permanently. All the following sections will form an internal document only and not for publication

17. The St Aloysius' College Historical Archives

Summarised pupil and staff files and other permitted categories of personal data form the basis of the formal records and the detailed historical archives of the St Aloysius' College and may be retained indefinitely for reference, historical and research purposes.

Personal data which is contained in the St Aloysius' College's archives may be processed for research purposes, (including statistical, historical or biographical purposes). Such processing will be carried out in such a manner as to comply with the Data Protection Principles, in so far as they may be applicable.

The St Aloysius' College reserves the right to destroy (in whole or in part) archived files whenever it considers it appropriate to do so.

18. Former Pupils and Alumni Development

Manual and computer-based files maintained in respect of current and former staff, pupils and other current, past and potential donors to the schools are to be kept securely. All access to such information held on computer is to be password protected.

Data will be used by the St Aloysius' College for a full range of activities, including the sending of school publications, promotion of benefits and services available to Former Pupils (including, if appropriate, those being made available by external organisations), notification of Former Pupils' activities and fundraising programmes (which might include an element of direct marketing).

Audit and Review of Policy

The implementation of this policy will be subject to periodic audit. The policy will be subject to review at three yearly intervals, or as and when pertinent legislation makes a review necessary.

Updated 24/08/15 JXC / KS
Legal Opinion edit 30/10/15
ARG edit 09/11/15

Appendix One

Data Protection Policy

Top tips on how to protect the personal data you hold.

For computer security:

- Ensure that there is a firewall and virus-checking on your computers.
- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Staff should only have access to the information they need to do their job and are not to share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.
- When leaving your computer unattended, even for a short time, the computer should be locked so that a third party cannot gain access to your data.
- All portable devices (smart phones, IPads etc.) on which work is performed must be password/pin number protected.
- All School data downloaded onto a USB Stick must be encrypted

For using emails securely:

- Consider whether the content of the email should be encrypted or password protected. The IT or security team should be able to assist you with encryption.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be very careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s arrangements are secure enough before sending your message.

For using faxes securely:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

For other security:

- Shred all your confidential paper waste.

- Check the physical security of your premises.

- Train your staff:

  - So they know what is expected of them;
  - To be wary of people who may try to trick them into giving out personal details;
  - So that they can be prosecuted if they deliberately give out personal details without permission;
  - To use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
  - Not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
  - Not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
  - Not to open spam – not even to unsubscribe or ask for no more mailings. Tell them to delete the email and either get spam filters on your computers or use an email provider that offers this service.

Appendix Two to
Data Protection Policy
Definitions

Personal data, as defined by the 1998 Act, is data which relates to a living individual who can be identified (a) from that data, or (b) from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. Personal data includes any expression of opinion about the individual and any indication of the intention of the Data Controller or any other person in respect of the individual.

Examples of personal data include:

- Name, age and date of birth of an individual
- Disciplinary records
- Annual appraisal
- An anonymised spreadsheet containing salary details and individual payroll numbers but where a separate document lists staff names and payroll numbers, allowing those individuals to be identified.

Data Controller, as defined by the 1998 Act, is a person or a body who determines the purpose which and the manner in which any personal data is to be processed.

Adequate level of protection, as defined in the 1998 Act, is one which is adequate in all the circumstances of the case, having regard in particular to –

- The nature of the personal data,
- The country or territory of origin of the information contained in the data,
- The country or territory of final destination of that information,
- The purposes for which and period during which the data are intended to be processed,
- The law in force in the country or territory in question,
- The international obligations of that country or territory,
- Any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
- Any security measures taken in respect of the data in that country or territory.

For further information on the Data Protection Act 1998, please turn to http://www.legislation.gov.uk/ukpga/1998/29/contents

For further information on your rights to make a subject access request, please turn to http://www.ico.gov.uk/for_the_public/personal_information.aspx