Data Protection Policy

inc. Acceptable Use Policy

Last reviewed - Oct 2014

St Julian's School

St Julian's School Data Protection Policy

St Julian's School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Fair Processing Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Commitment

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds

- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Headteacher, or nominated representative.

Contacts

If you have any enquires in relation to this policy, please contact **Rhys Evans (Acting Headteacher)** who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745

Appendix 1

St Julian's School

Procedures for responding to subject access requests made under the Data

Protection Act 1998

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to **Rhys Evans - Acting Headteacher** If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- ❏ passport
- ❏ driving licence
- ❏ utility bills with the current address
- ❏ Birth / Marriage certificate
- ❏ P45/P60
- ❏ Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependant upon the following:

- Should the information requested contain the educational record then the amount charged will be dependant upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days **(not working or school days but calendar days, irrespective of school holiday periods)**. However the 40 days will not commence until after receipt of fees or clarification of information sought.

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed,nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Acceptable Use Policy (AUP)

Staff

The computer system is owned by the school. It may be used by staff to enhance their professional activities including teaching, research, administration and management. The School's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.
The school reserves the right to examine or delete any files that may be held on its computer system or to monitor the Internet sites visited. The school reserves the right to withhold the privilege of Internet access to any person using the system inappropriately, either temporarily or permanently.

- All Internet activity should be appropriate to staff professional activity or education
- Access should only be made via the authorised school account and password
- Activity that threatens the integrity of the school ICT systems or activity that attacks or corrupts other systems is strictly forbidden
- Users are responsible for the content of all E-mail sent by them and for contacts made that may result in E-mail being received. If any appropriate E-mails are received then the individual's tutor/line manager should be informed
- Copyright material must be respected
- Posting anonymous letters, letters in someone else's name and forwarding chain letters is forbidden
- Use for personal financial gain, gambling, political purposes or advertising is strictly forbidden
- Use of school facilities to access inappropriate materials such as pornographic, racist, offensive or any illegal material is strictly forbidden
- Personal usage is not acceptable during lesson time

Social Media

Newport City Council wishes to ensure that use of social media does not expose the school to security risks or reputational damage.

The aim of this policy is to outline the responsibilities of employees using social media to ensure that staff do not put themselves in a vulnerable position when using social media, to ensure school information remains secure and is not compromised and to ensure the school's reputation is not damaged or adversely affected.
Examples of ways in which employees are linked to the school when they are using the Internet are (this list is not exhaustive):

- Using a school e-mail address as their contact e-mail address;
- Stating in their profile that they work for Newport City Council;
- Stating in a discussion online that they work for or with Newport City Council;
- Posting comments/information about the school on social networking sites;
- Joining/using a school managed social networking site;
- Accessing and using social media from school owned equipment (computers or smartphones).
- The school respects an employee's right to a private life. However, the school must also ensure that its reputation and confidentiality are protected. It must also try to ensure that employees are protecting themselves when using the Internet.

There are risks associated with using all different types of social media, such as:

- Disclosure of confidential information
- Damage to the reputation of the school
- Social engineering acts *(the act of manipulating people into disclosing confidential material or carrying out certain actions)*
- Civil or Criminal action relating to breaches of legislation
- Breach or Safeguarding
- Virus or other malware (malicious software) infection from infected sites or media
- In light of these risks, the school needs to ensure that the use of social media does not damage the school, its employees, partners or the people it serves.
- The school recognises that many employees may participate in social networking. When employees are using such sites and their use can be linked to Newport City Council, then the employee is deemed to be representing the school.

Employee Responsibilities

- Employees using social networking in a manner that can be seen as representing the school are required to:
- Ensure that they do not conduct themselves in a way that is and/or could be seen as bringing the school into disrepute;
- Ensure that any comments they post on any social networking site could not constitute bullying, harassment or discrimination;
- Never send abusive, defamatory or distasteful messages or post any potentially offensive images;
- Take care not to allow their interaction or any social networking site to damage working relationships with other school employees and/or school services users;
- Ensure that no information is made available that could provide a person with unauthorised access to the school, its systems and/or confidential information;
- Refrain from revealing any sensitive and/or confidential information regarding the school on any social networking website;
- Ensure that they do not contravene the Data Protection Act by posting information about the school, its employees or service users and must respect any copyright, fair-use and financial disclosure laws.
- Employees are reminded that the use of smartphones whilst at work, particularly for social media use, should be undertaken in their own time.

Personal Usage Guidance

If employees have personal profiles, they are reminded that the general public will be able to view their profile if it is set with public access, so they should take all appropriate steps to prevent themselves from revealing inappropriate or unprofessional information. It is highly recommended that employees review the privacy settings of their personal profiles and information, so that they control who they allow to see this information.

Employees must take care to consider the implications of accepting or inviting individuals that they are connected to as a result of their employment with the school (for example – a service user, school pupil, etc) to be a ‘friend’ on any personal social networking site. All communications with service users and pupils should be both professional and appropriate, both in and out of the work environment.

Employees are also advised to be security conscious and take steps to protects themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth, child's name, favourite football team, etc – or when they are away from home, which can form the basis of security questions and passwords.

_____
__

All files on the school's computer system will be regarded as public property. Regular checks may take place, to monitor the contents of email and web sites visited.

Declaration:
I have read the Terms and Conditions and understand and will abide by these. I further understand that violation of the regulations is unethical. Should I commit any violation, my access may be revoked.

User signature: _____ Print name:
_____

Date: _____