YSGOL STANWELL SCHOOL

Learning to Excel

Information Management and Governance Policy (IMAG)

GDPR Compliancy Policy May 2018

1 . INTRODUCTION

1.1 This policy is designed to ensure that the eight 'data protection principles' are observed to ensure that information is:

- used fairly and lawfully;
- used for limited, specifically stated purposes;
- used in a way that is adequate, relevant and not excessive;
- accurate;
- kept for no longer than is absolutely necessary;
- handled according to people's data protection rights;
- kept safe and secure;
- not transferred outside the European Economic Area without adequate protection.

1.2 The School is required to process personal data regarding staff, pupils and their parents / carers and shall take all reasonable steps to do so in accordance with this Policy. Processing amounts to collecting, using, disclosing, retaining or disposing of information. The data protection principles apply to all information held electronically or in structured paper files. The principles also extend to educational records – the names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, exam results, SEN assessments and staff development reviews.

1.3 In this Policy any reference to pupils, parents / carers, or staff includes current past or prospective pupils, parents / carers or staff.

1.4 All staff are responsible for complying with this policy.

2. SCOPE

2.1 This Policy covers the School's acquisition, handling and disposal of the personal and sensitive personal data it holds on all Staff, including temporary staff, agency workers, volunteers, parents and pupils. It also applies to Governors and contractors. It explains the School's general approach to data protection which is to ensure that individual's personal data and information is protected and appropriately processed and provides practical guidance which will help to ensure that the School complies with the Data Protection Act 1998 (the Act) and anticipates the **General Data Protection Regulations 2018** (GDPR) which becomes law on 25th May 2018.

3. DEFINITIONS

3.1 Personal data is:

- any information about a living person who can be identified (e.g. their name, address, online identifier such as an IP address, academics, school activities, attendance record, discipline, bank details and/or financial information in relations to parents and/or guardians, special education needs, exam results, images of students engaging in school activities, references or expressions of opinion about them). It makes no difference if they can be identified directly from the record itself or indirectly using other information in the School's possession or likely to come into the School's possession.
- personal information that has been, or will be, word processed or stored electronically (e.g. computer databases and CCTV recordings), personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g. name, school year, school activities). Rugby School Data Protection Policy – September 2017
- any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings.

The School has additional obligations in connection with the use of sensitive personal data, namely at least one of the following conditions must be satisfied:

- ✓ Explicit consent of the data subject must be obtained
- ✓ Necessary for carrying out the obligations under employment, social security or social protection law or a collective agreement
- ✓ Used in connection with ex-pupils / ex-staff provided it relates solely to them and there is no disclosure to a third party without consent
- ✓ Data manifestly made public by the data subject
- ✓ Various public interest situations as outlined in the General Data Protection

3.2 Sensitive personal data is:

- any information about a person's mental or physical health or condition, their political or religious beliefs, race, ethnicity, sexual life or orientation, trade union membership, criminal offences or alleged offences and any proceedings.

3.3 The data subject is:

- The person the information relates to. There may be more than one data subject, such as when a record concerns an incident involving two students.

3.4 The Data Controller:

- The School is the Data Controller and is responsible for determining the purposes of its use of data, what data it gathers and how this information is used. As the Data Controller the School is responsible for complying with the Act.

3.5 The Data Protection Officer:

- The School has appointed Mr J Mansfield as its Data Protection Officer, responsible for day to day compliance with this Policy. He can be contacted at Stanwell School, Archer Road, Penarth, CF64 2XL, by telephone on 029 20707633 or at school@stanwell.org.

4. ACQUIRING, USING AND DISPOSAL OF PERSONAL DATA

4.1 The School shall only process personal data for specific and legitimate purposes. These are:

- providing pupils and staff with a safe and secure environment, including images on CCTV. They are used for the purpose of detecting crime, ensuring personal security and the welfare of staff and pupils and the protection of the working environment. Images are kept no longer 28 days to meet these objectives, however, in certain circumstances such as an on-going investigation into criminal activity certain relevant images may be kept for longer but no longer than necessary to complete any such investigation.
- providing an education, staff training and pastoral care.
- providing activities for students and parents / carers: this includes school trips and activity clubs.
- providing academic, examination and career references for students and staff.
- protecting and promoting the interests and objectives of the School - this includes fundraising.
- safeguarding and promoting the welfare of pupils.
- monitoring pupils' and staff's email communications, internet and telephone use to ensure pupils and staff are following the Stanwell School's *IT Acceptable Use policy*.
- promoting the School to prospective pupils and their parents / carers.
- communicating with former pupils.
- for personnel, administrative and management purposes. For example, to pay staff and to monitor their performance.
- fulfilling the School's contractual and other legal obligations.

4.2 Staff should seek advice from the Data Protection Officer before using personal data for a purpose which is different from that for which it was originally acquired. If information has been obtained in confidence for one purpose, it shall not be used for any other purpose without the Data Protection Officer's permission.
4.3 The School shall not hold unnecessary personal data, but shall hold sufficient information for the purpose for which it is required. The School shall record that information accurately and shall take reasonable steps to keep it up-to-date. This includes an individual's contact and medical details.

4.4 The School shall not transfer personal data outside the European Economic Area (EEA) without the data subject's permission unless it is satisfied that the data subject's rights under the Act will be adequately protected and the transfer has been approved by the Data Protection Officer. This applies even if the transfer is to a pupil's parents or carers living outside the EEA**.**

4.5 When the School acquires personal information that will be kept as personal data, the School shall be fair to the data subject and fair to whoever provides the information (if that is someone else) in that their data will be handled and safeguarded in compliance with the Act.

4.6 The School shall only keep personal data for as long as is reasonably necessary and in accordance with the retention and disposal guidelines set out in the School's Document Retention Policy. Staff should not delete records containing personal data without authorisation.

4.7 The School will keep personal data secure and adopt technical and organisational measures to prevent unauthorised or unlawful processing of personal data.

INFORMATION AND EXPLANATION

5.1 Privacy Notice (Consent): Individuals must be told what data is collected about them, and what it is used for. This is called a privacy notice or Consent Form.

5.2 Purpose: The privacy notice / Consent Form is to ensure that the School's collection and processing of personal data is done in a transparent way so it will explain who it applies to, why the information is being collected, what information will be collected how it will be acquired and processed, what it will be used for, which third parties (if any) it will be shared with and outline the data subject's rights, including the right to complain about the processing of their data to the Information Commissioner's Office (ICO) at Wycliffe House, Water Lane, Wilmslow. Cheshire SK9 5AF, telephone 0303 123 1113 or at https://ico.org.uk/concerns/. This will include requesting permission for using pupils' images for school business.

5.3 Staff are not expected to routinely provide pupils, parents / carers and others with a privacy notice as this should have already been provided. Copies of the School's privacy notice for students and parents can be obtained from the Data Protection Officer or accessed on the School's website.

6. PROTECTING CONFIDENTIALITY

6.1 **Disclosing personal data within the School:**

- Personal data should only be shared on a need to know basis. Personal data shall not be disclosed to anyone who does not have the appropriate authority to receive such information, irrespective of their seniority within the School or their relationship to the data subject, unless they need to know it for a legitimate purpose.
- personal contact details for a member of staff (e.g. their home address and telephone number, and their private mobile telephone number and e-mail address) shall not be disclosed to parents, students or other members of staff unless the member of staff has given their permission.

6.2 Disclosing personal data outside of the School:

- Sharing personal data with others is often permissible so long as doing so is fair and lawful under the Act. However, staff should always speak to the Data Protection Officer if in doubt, or if staff are being asked to share personal data in a new way.

6.3 Before sharing personal data outside the School, particularly in response to telephone requests for personal data staff should:

- confirm the person phoning is legitimate by ending the call and phoning the relevant central switchboard asking to speak with the employee making the request;
- make sure they are allowed to share it – that they have the necessary consent;
- ensure adequate security. What is adequate will depend on the nature of the data. For example, pupil data should only be electronically transferred via the official channels of S2S, DEWI or *CHRONFA*; paper information should be sent by courier or recorded delivery, First or Second Class post is not considered secure enough; and
- make sure that the sharing is covered in the privacy notice.

6.4 The School should be conscious when using photographs, videos or other media as this is covered by the Act as well. Where images of pupils and/or staff are to be used publically, alongside their name, consent from the relevant parties should be sought on each occasion irrespective of whether the Consent Form has given permission to use pupil photographs.

6.5 Information security and protecting personal data:

The School shall do all that is reasonable to ensure that personal data is not lost or damaged, or accessed or used without proper authority, and the School shall take appropriate steps to prevent these events happening. In particular:

- paper records which include confidential information shall be kept in a cabinet or office which is kept locked when unattended.
- the School uses a range of measures to protect personal data stored on computers, including file encryption, anti-virus and security software, sufficiently robust and frequently changed user passwords, audit trails and back-up systems.
- staff must not remove personal data from the School's premises unless it is stored in an encrypted form on a password protected computer or memory device.
- staff must **not** use or leave computers, memory devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: they should not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

7. **DATA BREACHES**

7.1 Definition: A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure or access to personal data.

7.2 Reporting obligations: Any actual data breach or alleged data breach must be reported to the Data Protection Officer as soon as it is discovered, whatever time that might be, to enable its circumstances to be investigated and appropriate action taken to limit any damage and to prevent a similar occurrence.

As soon as the School becomes aware of a significant data breach as determined by the Data Protection Officer it has 72 hours in which to report the breach to the Information Commissioner's Office (ICO). Examples of breaches and their seriousness for reporting purposes are:

- mistakenly sending an email containing personal data to an incorrect recipient.
- loss or theft of IT equipment containing personal data.
- loss or theft of hard copies of data files
- failing to deal with a Subject Access Request.

When considering if a breach is serious the Data Protection Officer must consider if the breach is likely to result in a high risk to the rights and freedoms of individuals: e.g. resulting in discrimination, damage to reputation, financial loss – through identity theft or otherwise – loss of confidentiality or any other significant economic or social disadvantage. If this is deemed to be the case not only does this breach have to be reported to the ICO within 72 hours of its discovery, the individuals concerned must be notified of the breach in a timely manner as directed by the Data Protection Officer.

8. DATA SUBJECT'S RIGHTS, INCLUDING SUBJECT ACCESS REQUESTS (SAR)

8.1 Individuals are entitled to know whether the School is holding any personal data which relates to them, what that information is, the source of the information, how the School uses it and who it has been disclosed to. This is known as a Subject Access Request.
Any member of staff wishing to exercise the right to request information covered by this policy, can do so by submitting a request in writing to the Data Protection Officer.
Any member of staff who receives a request for information covered by this policy from a pupil, parent / carer or any other individual must inform the Data Protection Officer as soon as is reasonably possible, normally on the same day. This is important as there is a statutory procedure and timetable which the School must follow. The School has only 30 days' to respond to a Subject Access Request from whenever the request is received.

8.2 Individuals have a right to ask the School not to use their personal data for direct marketing purposes or in ways which are likely to cause substantial damage or distress.

8.3 Individuals have a right to ask for incorrect personal data to be corrected or annotated.

8.4 Individuals have the right to object to any of their personal data being processed and to have this data erased.

8.5 Individuals have the right to restrict (halt) the processing of their personal data, usually whilst incorrect data is being corrected.
8.6 Individuals have the right to request their personal data is transferred to another data controller in a commonly used format.

8.7 Individuals have a right to ask the School not to make automatic decisions (using personal data) if such automatic decisions would affect them to a significant degree.

8.8 Individuals have the right to complain about the processing of their personal data to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, Telephone 0303 123 1113 or at: https://ico.org.uk/concerns/.

9 .FURTHER INFORMATION

9.1 The School has registered its use of personal data with the Information Commissioner's Office and further details of the Personal Data it holds, and how it is used, can be found in the School's register entry on the Information Commissioner's website at www.ico.gov.uk under registration number Z6175287. This website also contains further information about data protection.

10 BREACH OF THIS POLICY

10.1 A member of staff who deliberately or recklessly discloses personal data held by the School without proper authority is potentially guilty of a criminal offence and gross misconduct. In the case of a serious breach, summary dismissal will be considered.

11. STATUS

11.1 This policy is intended only as a statement of School policy. It does not form part of the contract of employment and may be amended from time to time.

RELATED POLICIES
Discipline Policy
IT Acceptable Use Policy
Privacy Notice / Consent Form for Staff (Staff Handbook)
Privacy Notice / Consent Form for Pupils and Parents

12. FURTHER INFORMATION

12.1 Further information and guidance regarding this policy or its application can be obtained from the Data Protection Officer.

Date: 2nd February 2018

Date Reviewed: