Parkstone Grammar School

PERSONAL INFORMATION HANDLING POLICY AND PROCEDURES

Date approved:	**21st March 2017**
Approved by:	Personnel and Finance committee
Date of next review:	2019-20
Type of policy	Statutory

PERSONAL
INFORMATION HANDLING

INTRODUCTION

The school needs to collect and use certain types of information about students, their families, and members of the Governing Body, employees and those with whom it deals in order to perform its functions. This includes information on current, past and prospective employees, students, persons with parental responsibility, suppliers, customers, service users and others with whom it communicates. The school is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of the Government. Schools have always held personal data on the students in their care, and increasingly this data is held digitally and accessible not just in school but also from remote locations.

It is important to stress that this policy applies to all forms of personal data, regardless of whether it is held on paper or in electronic format.

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include (but is not limited to) :

- Personal information about members of the school community – including students, members of staff and parents and carers eg names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Curricular / academic data eg class lists, student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members

POLICY AIMS

This policy outlines the school's arrangements for ensuring, as far as possible, the safety and security of any material of a personal or sensitive nature. It also outlines the arrangements for access to personal information by students, persons with parental responsibility, employees and members of the public in accordance with The Data Protection Act 1998 (DPA).

This policy will be communicated to all employees and will be published to employees through the school's normal channels and will be available on the school's website.

The policy applies to all personal information held by the school irrespective of ownership of the data. Personal information is defined for the purposes of this policy as being any information from which an individual can be identified (including pictures, CCTV images, voice, etc.).

POLICY OBJECTIVES

This policy outlines the school's approach to ensuring all employees effectively process and manage personal information within set standards, to protect the privacy of individuals, and to comply with the principles and requirements of the DPA and other legislation. This Personal Information Handling Policy informs employees on procedures that comply with the DPA when handling personal information about students, parents, visitors, clients, contractors and employees.

This policy should be complied with for personal information relating to all individuals whether deceased or living.

This policy should be read in conjunction with The Bournemouth, Dorset and Poole Children and Young People's Partnerships Multi-Agency Data and Information Sharing Protocol.

The policy covers requests for information from individuals for their own personal data. Such requests, defined as subject access requests (SAR), should be handled in accordance with this policy, in compliance with the Data Protection Act 1998.

A definition of terms is available at Appendix A.

Objectives:

- To promote the effective, consistent and legal processing of personal information by defining a Personal Information Handling Policy.
- To ensure that all employees are aware of their responsibilities in relation to the processing of personal information and to the law surrounding its use.
- To ensure that all employees are aware of the consequences of the misuse or abuse of personal information.
- To establish and maintain trust and confidence in the school's ability to process personal information.
- To ensure compliance with legislation, guidance and standards relating to the handling of personal information.

SAFEGUARDING

The school is committed to safeguarding staff and students against the misuse of personal information which may cause harm. The school will ensure that all information is protected appropriately and only shared in accordance with this policy.

EQUAL OPPORTUNITIES

The school believes that every student has the right to attend school and receive a high-quality education. Therefore any and all personal information will only be used to this end.

CORE SCHOOL VALUES

The school believes in providing a safe and secure environment in which our young people can thrive and in positive home school relations and the secure protection and transfer of information is important to secure this aim.

LINKED POLICIES

- Data Protection Policy
- Equality Policy

WHAT KEY ACTIONS IS THE SCHOOL TAKING TO ENFORCE THIS POLICY?

The policy will be reviewed regularly by the Governing Body to take into account changes in legislation and to ensure that it remains timely and relevant. Any changes will be publicised through normal communication channels.

The effectiveness of the policy will also be assessed through the monitoring of requests for personal information, the school's responses to these, and concerns/complaints. These events will be collated into an annual report presented to the Governing Body. Where issues of concern arise, then appropriate advice will be obtained.

The policy will be published on the school's web site.

An information audit may be conducted every three years by the school's administration team and any recommendations complied with, within agreed timescales. This also complies with Section 46 of the Freedom of Information Act.

WHAT AREAS ARE COVERED IN THE POLICY? PROCEDURE

The school regards the lawful and correct treatment of personal information as critical to successful operations, and to maintaining confidence between those with whom the school deals. It is essential that the school treats personal information lawfully and correctly.

The purpose of the Data Protection Act 1998 is to protect the rights and privacy of living individuals. It regulates the processing of personal information including the obtaining, holding, use or disclosure of such information. It places obligations on those who record and use personal information and gives rights to those whose information is being processed.

Information will be retained at Parkstone Grammar School in the format established by the "Information and Records Management Society Retention Guidelines for Schools" document that can be found http://www.irms.org.uk/groups/public-sector/resources/134-records-management-toolkit-for-schools.

PROCESSING PERSONAL INFORMATION

The processing of personal information is defined as encompassing everything that we do with personal information including the sharing, transferring or disclosing of personal information to another organisation or internally.

Personal information must be processed in accordance with the eight principles under the Data Protection Act 1998 unless an exemption applies.

A checklist of "good practice" is given as Appendix B.

Employees must respect personal information that they have access to and treat it in the manner in which they would expect their personal details to be treated.

Employees must have regard and respect for the privacy of students, persons with parental responsibility and employees and process their personal information accordingly.

Access to personal information must be accepted by all to be on a need as well as a right to know basis.

Personal information will be held securely, and accessible only by those with a need and a right to know. The Headteacher is responsible for ensuring that personal information is protected by appropriate levels of security, i.e. relevant to the sensitivity of the personal information being processed.

Arrangements and contingencies need to be in place in order to protect personal information from loss due to natural disaster and the actions of third parties e.g. flood, arson, theft.

Personal information must not be transmitted or transported externally via manual or electronic means without appropriate security. Portable devices (laptops, iPads, CDs, DVDs, USB memory sticks, etc) which contain personal information will use adequate security measures e.g. password / encryption, to protect against losses or access by unauthorised persons. Staff wishing to work on personal information externally should request clearance from the Headteacher and ensure that security measures are in place before such information is transferred. The DfE requests that no identifiable COLLECT information will be accessed by laptop unless encrypted. This is because COLLECT data is the responsibility of the DfE. Any laptop containing sensitive data could be lost, or could be seen by unauthorised people if the laptop is used outside the school.
Personal information must be disposed of safely and securely when it has reached the end of its shelf-life.

Personal information will not be passed on to any third party unless any one or more of the following apply (Schedules 2 & 3 of the Data Protection Act):

- permission or consent is obtained from the data subject or in the case of minors, parents;
- the organisation requesting the information has a legal right to the information (e.g. police investigating crime);
- it is a requirement of law;
- it is to comply with a court order;

- it is necessary to provide educational services;
- the school reasonably believes it is in the subject's own interest;
- the school reasonably believes it is in the overall public interest and in a particular instance this is judged to outweigh the other considerations.

At the point of collection the data subject will be informed of the purposes for which the information is being collected and processed together with any other relevant details regarding this processing. At this time, where choices are available the student or persons with parental responsibility will be given the opportunity to opt out of the school's non-statutory information processing arrangements, e.g. by withholding consent to the taking of images for publicity purposes.

The school will promote good practice in the sharing of information with its partners, Government agencies and departments and other public and private sector organisations. All sharing will comply with the Data Protection Act 1998 and the Information Sharing Guidance.

The quality and accuracy of personal information should be relevant to the purpose for which it is to be used.

The purposes for which personal information are processed in the school will be detailed in the school's Fair Processing Notice which will be renewed regularly with the Information Commissioner's Office. Any changes to purposes must be identified to the school's Information and Security Officer (ISO) who will submit amendments as required, e.g. if the school decided to install CCTV cameras.

Processing of information for a purpose not reflected in the Data Protection Act 1998 or in the notification must be approved by the ISO.

Complaints regarding the handling or processing of personal information should be referred to the ISO.

Any inaccurate or misleading information will be checked and corrected as soon as the student or parent brings this to the school's attention.

The rights of data subjects as defined by the Data Protection Act 1998 and specifically their right of access to their own personal information will be complied with fully and given appropriate respect and priority.

THE SUBJECT ACCESS REQUEST PROCEDURE

Requests by individuals (or their representative) for copies of their own information **must be in writing** and supported by significant proof of identity. The following originals (not photocopies) are suggested:

- passport;
- driving license;
- birth/marriage certificate

The need to check and verify the identity of the requester can be particularly important where that

person is a child or someone is purportedly making the request on behalf or in respect of a child. Whereas a utility bill can help, it is not felt to be 100% secure. In cases of doubt the school will seek assistance from the ISO.

All requests for personal information must be passed to the school's ISO.

Requests for personal information will be recorded and monitored by the ISO.

The decision on whether to release information in the event of a request will be taken by the Headteacher, in collaboration with the ISO. This is also to ensure compliance within timescales.

Information must not be deleted or disposed of, after the receipt of a request, unless requested by the subject. Subjects have the right to have incorrect or inaccurate information corrected.

Subject Access Requests will be supplied within **15 school days for students** and **40 days for employees**. Where an investigation of a member of staff has commenced and Subject Access has been requested by that member of staff, the processing of the request should be undertaken as quickly as possible. In the event that a complaint is received regarding a Subject Access Request, the complaint will be addressed by the Governing Body following the school's Complaints Procedure. The Information Security Officer will be informed at the earliest opportunity if the school receives a complaint. Records of proceedings and decisions made will be kept in order to provide evidence for any external review of the complaint by the Information Commissioner's Office.

TRAINING

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities through:

- Induction training for new staff
- Staff Meetings/Briefings/INSET
- Day to day support and guidance from the Leadership Group

The Headteacher and Leadership Group are responsible for ensuring that all employees receive personal information handling training appropriate to their responsibilities.

CHARGING

Requests for copies and access to personal information held by the school will incur a charge of £10 for the processing of a request. The required proof of identity of the requestor (with written consent of the data subject if requesting on behalf of a student over the age of 12 years) must be received prior to processing the request and the start of the 15 or 40 days response deadline (whichever applies). There may be a charge for disbursements i.e. printing, postage and packing.

Employees requiring access to their own personal information held by and on behalf of the school will also be charged and charges for disbursements may be applied.

Requests for personal information held by the school about an individual may result in the school seeking clarification from the requestor, for example to specify an area of information required, services

or timescales. In cases where clarification is sought, the clock stops until the clarification is received and then restarts from where it left off.

INAPPROPRIATE AND UNACCEPTABLE USE

Everyone in the school has the responsibility for handling protected or sensitive data in a safe and secure manner and to avoid any inappropriate and unacceptable use.

Unacceptable use includes:

- unauthorised access to personal information;
- unauthorised disclosure of personal information;
- unauthorised use of personal information, e.g. use of which the data subject has not been informed/consented to (as in Sections 2 & 3 of the Data Protection Act 1998 and the Fair Processing Notice); and
- non-adherence to the school's policies

Employee, client or student personal information must not be used for:

- any illegal purpose;
- any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the school into disrepute; or
- any purpose which is not in accordance with the employee's role or job description.

(This is not an exhaustive list).

Employees are required to notify an appropriate manager, or the Information Security Officer, if they become aware, or suspect that personal information is being misused or handled inappropriately.

NON-COMPLIANCE WITH THE LEGISLATION AND POLICY

The Headteacher and Governing Body are responsible for ensuring that employees' responses to requests for personal information remain appropriate and are in accordance with this policy and the Data Protection Act 1998.

The Headteacher and Governing Body must ensure that instructions given to employees, relating to requests for personal information and the processing of personal information, comply with any legislation and/or school policy.

The School will have arrangements in place that avoid parental and visitor contact with personal information to which they do not have a right.

All employees must be aware of their own obligations with regard to the disclosure and the processing of personal information.

Employees not complying with this policy or legislation may be subject to the school's Disciplinary Procedures. In the event of non-compliance by an agency worker, casual worker or contractor, his/her work with the School may also be reviewed under the school's Disciplinary Procedures, depending upon the circumstances of the case.

WHAT MUST EVERYONE DO TO UPHOLD AND ENFORCE THE POLICY?

GOVERNORS

- Ensure that information handling is given a high priority in the school and is included in the strategic improvement plan if necessary.
- Governors should agree and approve the Information Handling Policy.
- Governors should monitor and evaluate information handling and the school's work to ensure safe storage and communication of information.

HEADTEACHER / LG

- Formulate the draft Information Handling Policy
- Ensure a leadership structure is in place to promote safe Information Handling
- Be vigilant in cases of information breaches
- Report to governors on breaches.

STAFF

- Staff should set an example in information handling and sharing

PARENTS

- Parents should encourage and facilitate safe communication of information and update the school when contact details change

WHO SHOULD PEOPLE CONTACT IF THEY HAVE A QUESTION ABOUT THIS POLICY OR A SUGGESTION FOR IMPROVEMENT?

Information Security Officer (Tracy Harris)
Parkstone Grammar School
Sopers Lane
Poole BH17 7EP

The Information Commissioner's Office (ICO) Tel: 08456 30 60 60
01625 54 57 45 Fax: 01625 524510

Press and Media Enquiries: Tel: 020 7025 7580
http://www.ico.gov.uk/

By Post: The Information Commissioner's Office, Wycliffe House, Water lane, Wilmslow, SK9 5AF

By email: If your enquiry is about a new or existing notification under the Data protection Act, please email notification@ico.gsi,gov.uk. You may find it helpful to read more about notification and the need to notify before sending your enquiry.

APPENDIX A

DEFINITIONS

a)	**Personal Information**
	Information relating to a living individual who can be identified from that information and other information in possession of the organisation. This is information that affects a person's privacy whether in their personal or family life, business or professional capacity and includes the name, address and telephone number of an individual. It will also include information on a person's medical history, an individual's salary details and includes expression of opinion about the individual and of the intentions of the organisation in respect of that individual. Personal information also includes CCTV images and photographs which enable the identification of an individual.
b)	**Sensitive Personal Information**
	Is defined in the Act as racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sex life, criminal convictions.
c)	**Data Subject**
	Any living individual who is the subject of personal information held by an organisation. E.g. a student, parent, member of school staff, member of the public, partnership worker, councillor.
d)	**Processing**
	Any operation relating to information including: organising, retrieving, disclosing or otherwise making information available, deleting, obtaining, recording, altering, adding to or merging.
e)	**Third party**
	Any individual or organisation other than the information subject, the information controller or its employees or agents.

APPENDIX B

Procedures for the Secure Handling of Personal Information

Procedures in the context of this Policy cover:

- Fax
- Paper records
- E-mail/computer
- Telephone/Spoken communication
- Post/Informal messages e.g. post-it notes/telephone message notes

Best Practice Checklist

Fax machines

- Ensure fax equipment is sited where unauthorised people cannot access it
- When sending information by fax, do not include personal details unless absolutely necessary
- Programme numbers into the fax machine memory to avoid misdialling.
- Confirm the fax number before sending.
- Check that recipient is waiting to receive a confidential fax
- Always use an official fax header with a confidentiality statement printed on it

Paper records and files

- All paper records containing personal and/or confidential information must be maintained and handled securely
- Effective security must be maintained when personal and/or confidential information is being transferred or taken out of a secure environment
- Any loss of personal and/or confidential records must be reported immediately to a member of the Leadership Group

E-mail and computer use

- Only use electronic mail in accordance with school policy
- Do not send external emails containing confidential and/or personal information unless suitable encryption facilities are available
- Ensure that computer screens showing confidential and/or personal information cannot be seen by unauthorised people
- Ensure that passwords are maintained securely, not shared with others and changed regularly
- Ensure that all personal information stored is accurate
- Only record information that is relevant and remember that an individual has a right of access to their personal information

Telephone & verbal communication

- Check to see whether confidential conversations may be overheard and take steps to ensure that they are not
- When discussing confidential information using the telephone you must be confident that the person on the other end should be receiving the information
- Avoid sharing confidential information in public places, e.g. reception desk, corridors

Post, informal messages and notes

- Check addresses are up to date and ensure that letters are addressed correctly
- Always seal envelopes containing confidential information
- Destroy in a secure manner, all informal or 'short shelf life' information which is no longer required, e.g. post-it notes, telephone messages

General

- Ensure that visitors are not able to access confidential information
- All contractors have a contractual obligation to maintain confidentiality, but access to sensitive personal data should be restricted where practicable
- Take care when releasing information to relatives, e.g. giving information to separated parents about students

This list is not definitive, but highlights some areas of best practice.