John Willmott School - Personal Data Handling Policy

Introduction

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data to ensure that it cannot be accessed by anyone who does not:

- Have permission to access that data
- Need to have access to that data

Data breaches can have serious effects on the individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function, it will not hold it for longer than is necessary and only use it for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. 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:

- Personal information about members of the school community – including students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, student progress records, reports, references
- Professional records e.g. 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

Responsibilities

The school's Senior Information Risk Officer (SIRO) is The Director of Support Services. This person will keep up to date with current legislation and guidance and will:

- Determine and take responsibility for the school's information risk policy and risk assessment
- Appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- What information is held, for how long and for what purpose
- How information has been amended or added to over time
- Who has access to protected data and why

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (e.g. LA, DfE, etc.) to whom it may be passed.

This privacy notice will be passed to parents / carers through the school website www.jws.bham.sch.uk. Parents / carers of students who are new to the school will be provided with the privacy notice through the school website.

Training & Awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff Meetings / Briefings / Inset
- Day to day support and guidance from Information Asset Owners, Director of Support Services

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present
- Judging the level of the risks (both the likelihood and consequences)
- Prioritising the risks

Risk assessments are an on-going process and should result in the completion of an Information Risk Actions Form (sample below):

Risk ID	Information Asset Affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall Risk Level (Low, Medium, High)	Action(s) to Minimise Risk

Impact Levels and Protective Marking

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protected, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach.

A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g. "Securely delete or shred this information when you have finished using it".

Secure Storage of and Access to Data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods).

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off site backups of Management Information System Data.

All paper based Protected and Restricted (or higher) material must be held in lockable storage.

The school recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access.

Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject.

Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them.

Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure Transfer of Data and Access Out of School

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.

- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) when out of school.

- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.

- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.

- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (To carry encrypted material is illegal in some countries)

Disposal of Data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals, Director of Support Services, Senior Office Manager.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy.

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- A "responsible person" for each incident
- A communications plan, including escalation procedure
- A plan of action for rapid resolution
- A plan of action of non-recurrence and further awareness raising

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of Technologies and Protective Marking

	The Information	The Technology	Notes on Protect Markings (Impact Level)
School Life and Events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of students work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and Achievement	Individual student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this student record available in this way.
Messages and Alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Privacy Notice

Privacy Notice - Data Protection Act 1998

We John Willmott School are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support Your Teaching and Learning
- Monitor and Report on Your Progress
- Provide Appropriate Pastoral Care
- Assess How Well Your School is Doing

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your and your parent(s) name(s) and address, and any further information relevant to the support services' role. However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service. Please inform the Senior Office Manager if you wish to opt-out of this arrangement. For more information about young peoples' services, please go to the Direct.gov Young People page at www.direct.gov.uk/en/YoungPeople/index.htm.

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE).

If you want to see a copy of the information about you that we hold and/or share, please contact The Headteacher.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

http://www.birmingham.gov.uk/schools

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

- Information Officer, Birmingham City Council (0121 464 4591)

- Public Communications Unit
  Department for Education
  Sanctuary Buildings
  Great Smith Street
  London
  SW1P 3BT

  Website: www.education.gov.uk
  Email: http://www.education.gov.uk/help/contactus
  Telephone: 0370 000 2288