Osmani Primary School

Reach For The Stars

Data Protection Policy

Last review date: Spring 2016
Next review date: Spring 2018

1. At Osmani, we value:

1. Difference and respect each other
2. Health and Wellbeing
3. High aspirations and enjoyment of learning
4. Honest feedback to one another
5. Supporting and empowering each other

2. SCHOOL VISION STATEMENT

Our purpose is to develop an inclusive school, which promotes and achieves excellence, and continues to nurture the values, confidence and skills of pupils, staff and the community, in order to meet the emerging opportunities of the 21st century.

3. Therefore we aim to:

Foster the enjoyment of learning by

- having the highest expectations of achievement
- providing a broad, balanced and enriched curriculum
- teaching and learning in varied and creative ways
- encouraging talking, questioning, curious and open minds
- being open to change and innovation in order to improve

Promote the health and wellbeing of all by

- valuing everyone equally and believing that everyone is important
- giving everyone the opportunities to develop their potential
- supporting and promoting a safe and healthy lifestyle
- having the highest expectations of behaviour
- developing high quality relationships between all members of the school community

Promote a collaborative community by

- valuing our differences and learning from each other
- listening to each other and working co-operatively in groups and teams
- working with our parents and carers, other schools, organisations, businesses, local, national and international communities
- letting each other know how well we are doing and how to do even better

Last review date: Spring 2016

Next review date: Spring 2018

Prepare for our future wellbeing by

- caring for the school environment and the wider environment
- thinking about the future and our roles and responsibilities as citizens
- being ready for opportunities and challenges
- aiming to become life-long learner

Equal Opportunities and the Single Equality Scheme

We believe that all those who work in Osmani - children and adults - have the right to be treated fairly and with respect by everyone connected with the school.
We aim for Osmani to be a safe, supportive place, where all children and adults feel valued as individuals, whatever their **ability, age, disability, gender reassignment, marriage or civil partnership, pregnancy & maternity, race, religion or belief, sex and sexual orientation.**
The school aims to foster the social and personal skills of co-operation, sharing and mutual respect.

Summary
Introduction

The objectives of this Policy, which is intended for all school staff, including governors , who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

Definitions

Information - covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

Personal Data - Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on. It applies only to that data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'. This includes paper filing systems.

Last review date: Spring 2016
Next review date: Spring 2018

Strong Password – Password which is 8 characters minimum length, contains upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain dictionary words, the owner's date of birth or car registration number.

Encryption – Process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Osmani Primary School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Osmani Primary School must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.

Osmani Primary School and all staff or others who process or use personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the School has developed this Data Protection Policy.

Status of this policy

This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the School from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.

The Data Controller and the Designated Data Controllers

Last review date: Spring 2016

Next review date: Spring 2018

The School as a body corporate is the Data Controller under the 1998 Act, and the Governors are therefore ultimately responsible for implementation. However, the Designated Data Controllers will deal with day to day matters.

The School has three Designated Data Controllers: They are the Headteacher, the School Business Manager and the Administrative Officer.

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Lead Designated Data Controller, who would be:
School Business Manager

Responsibilities of Staff

All staff are responsible for:

- Checking that any information that they provide to the School in connection with their employment is accurate and up to date.

- Informing the School of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the School of such changes.

- If and when, as part of their responsibilities, staff collect information about other people(e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff set out in the Schools Data Protection Code of Practice.

Responsibilities:

- The School shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act.
- Users of the school's ICT systems and data must comply with the requirements of the ICT Security Policy.
- The School's Leadership Group shall review this document at least annually.
- Users shall be responsible for notifying the System Manager and Headteacher of any suspected or actual breach of ICT security.
- ***The Headteacher shall inform both the ICO and the LA if there are any losses of personal data***
- Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.

Last review date: Spring 2016

Next review date: Spring 2018

- Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- Adequate procedures must be established in respect of the ICT security implications of personnel changes.
- No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, external hard disks, memory sticks and Personal Digital Assistants (PDAs) & other removable media.
- Remote access to information and personal data shall only be provided through an encrypted link and users shall require a strong password that is renewed at least termly.
- Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web sites including the Learning Platforms unless these documents are encrypted.

Data Security
Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

All staff are responsible for ensuring that:

- Any personal data that they hold is kept securely.

- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Personal information should:

- Be kept in a locked filing cabinet, drawer, or safe; or

- If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and

- If a copy is kept on a removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
-

Last review date: Spring 2016
Next review date: Spring 2018

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

This Policy document and the School's Data Protection Code of Practice address in particular the last three points above. To address the first point, the School will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should complete the *Subject Access Request* Form and submit it to the Designated Data Controller. **(Appendix 1)**

The School will make a charge of £10 on each occasion that access is requested, although the School has discretion to waive this.

The School aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days, as required by the 1998 Act.

Subject Consent

In many cases, the School can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the 1998 Act, express consent must be

Last review date: Spring 2016

Next review date: Spring 2018

obtained. Agreement to the School processing some specified classes of personal data is a condition of acceptance of employment for staff. This included information about previous criminal convictions.

Jobs will bring the applicants into contact with children. The School has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The School has a duty of care to all staff and students and must therefore make sure that employees and those who use School facilities do not pose a threat or danger to other users. The School may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The School will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This may be to ensure that the School is a safe place for everyone, or to operate other School policies, such as the Sick Pay Policy or the Equal Opportunities Policy. Because this information is considered **sensitive** under the 1998 Act, staff (and students where appropriate) will be asked to give their express consent for the School to process this data. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Publication of School Information

Certain items of information relating to School staff will be made available via searchable directories on the public Web site, in order to meet the legitimate needs of researchers, visitors and enquirers seeking to make contact with the School.

Retention of Data

The School has a duty to retain some staff and student personal data for a period of time following their departure from the School, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time.

Physical Security:

- As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.

Last review date: Spring 2016

Next review date: Spring 2018

- Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- All school owned ICT equipment and software should be recorded and an inventory maintained.
- Uninterpretable Power Supply (UPS) units are recommended for servers and network cabinets.
- Computer monitors should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.
- **Do not** leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- **Do not** give out sensitive information unless the recipient is authorised to receive it.
- **Do not** send sensitive/personal information via e-mail or post without suitable security measures being applied.
- Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security:

- Users **shall not** make, distribute or use unlicensed software or data.
- Users **shall not** make or send threatening, offensive or harassing messages.
- Users **shall not** create, possess or distribute obscene material.
- Users must ensure they have authorisation for private use of the school's computer facilities.
- Passwords should be memorised. If passwords must be written down they should be kept in a secure location.
- Users who regularly access personal data shall have a unique user ID and a strong password that is renewed at least termly
- Passwords **shall not** be revealed to unauthorised persons.
- Passwords **shall not** be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data.
- Passwords shall be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- Regular backups of data, are taken every day onto removable hard disks and rotated weekly, as part of a maintenance strategy
- Data designated critical or sensitive are encrypted and is backed up off site using SSL with 1024 bit RSA key exchange, 128 bit RC5 stream cipher and SHA-1 integrity checking.
- Security copies are regularly tested to ensure they enable data restoration in the event of system failure.
- Security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection:

- The school should ensure current and up to date anti-virus software is applied to all school ICT systems.

Last review date: Spring 2016

Next review date: Spring 2018

- Laptop users shall ensure they update their virus protection at least weekly.
- Any suspected or actual virus infection must be reported immediately to the System Manager/ICT Co-ordinator and that computer shall not be reconnected to the school network until the infection is removed.

Disposal of Equipment:

- The School shall ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- It is important to ensure that any software remaining on a PC being relinquished for reuse are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The School shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

Conclusion

Compliance with the 1998 Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Appendix 1

Last review date: Spring 2016
Next review date: Spring 2018

ACCESS TO PERSONAL DATA REQUEST

DATA PROTECTION ACT 1998 Section 7.

Enquirer's Surname ……

Enquirer's Forenames ……

Enquirer's Address ……

……

……

……

Enquirer's Postcode ……

Telephone Number ……

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")? YES / NO

If NO,

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? YES / NO

If YES,

Name of child or children whose personal data records you are making an enquiry about.

……

……

……

……

Last review date: Spring 2016
Next review date: Spring 2018

Description of Concern / Area of Concern

Description of Information or Topic(s) Requested (In your own words)

Additional information.

Last review date: Spring 2016
Next review date: Spring 2018

Please despatch / reply to: *(if different from enquirer's details as stated on this form)*

Surname ……

Forenames ……

Address ……

……

……

……

Postcode ……

Telephone Number …….

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address
(or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent)

……

Name of "Data Subject" (or Subject's Parent) (PLEASE PRINT)

……

Date

Last review date: Spring 2016
Next review date: Spring 2018

Last review date: Spring 2016
Next review date: Spring 2018

Last review date: Spring 2016
Next review date: Spring 2018

Last review date: Spring 2016
Next review date: Spring 2018