Data Security Policy 2012-2013

Introduction

The purpose of this document is to ensure that all users and keepers of data (Staff, Pupils and Temporary Staff) of Ruislip Gardens Primary School are aware of the rules regarding personal data and the Freedom of Information Act 2000. It is the responsibility of all users and keepers of data in Ruislip Gardens Primary School to be aware of and follow all school data policies and guidelines and to seek advice in case of doubt. This policy may be updated or supplemented by specific standards or procedures to reflect further developments in technology or legislation or other relevant changes.

The following terminology will be used throughout this document:

- Personal data – data relating to any living individual, or from which a living individual can be identified; this can take the form of electronic or manual records as well as photographic and CCTV images.
- Sensitive personal data – personal data relating to an individual's mental or physical health, race/ethnic origin, religious or political beliefs, sex life or trade union membership.
- Data subject – an individual to whom any personal data relates.
- Data controller – any organisation that is responsible for processing personal data.
- Data processor – any organisation that processes personal data on behalf of a data controller.

These definitions and much of the other material in this document is adapted from the BECTA ICT Advice document "Data Protection and Security, a summary for schools" (2004). The Copyright in this document is held by BECTA and its use is gratefully acknowledged.

Specific guidance on the use of photographs in school can be obtained from the Information Commissioner's Office web site www.ico.gov.uk

Data security

Users must only access data held on Ruislip Gardens Primary School's computer systems if they have been properly authorised to do so. Shared data areas on the server exist where staff are required to share files, carry out work or contribute to project collaborations. If there is any doubt about access rights to any data area, please contact Admin Officer/or the Project Coordinator responsible for the data to be accessed. It is school policy for users to store data on a network drive where it is regularly backed up.

Staff with laptops must remember that data from their network "home" drive is synchronised with their laptop. If the laptop is stolen, this could lead to data falling into unauthorised hands. Staff must ensure that their laptop access is protected by a strong password (see Password Policy) and must store only data which is needed at home in this area. The hard drive of all laptops taken home must have additional security encryption software. If in doubt ask the school technician.

Some staff members are issued with memory sticks. The data on these sticks should be encrypted.

When reporting a laptop theft, the member of staff must provide a list of all personal data or sensitive personal data held.

Under no circumstances should any user disclose personal or other confidential information held on computer to unauthorised persons. The unauthorised access to and/or unauthorised modification of data is a criminal offence under the Computers' Misuse Act 1990.

In particular, no person may use the school SIMS system or any other central database, to extract data via a report or by hand, using electronic means, photographic means or paper and then use the data or allow it to be used away from the school premises without the express consent of the Head Teacher. This applies even if the person is authorised to view the data in school.

Staff should note that all data and correspondence, including e-mail messages, held by Ruislip Gardens Primary School (including that on school laptops) may be provided to a data audit, internal or external, in the event of an audit access request.

Email

Ruislip Gardens Primary School issues email addresses to all staff. Staff addresses follow a predictable pattern. This is a requirement of the Hillingdongrid Email system. The email user must be consulted before their email address is passed on to anyone else.
The children also have email addresses allocated although only Y3, Y4, Y5 and Y6 are made aware of this.

School Website

Ruislip Gardens Primary School has a website which is used to pass on information to parents and others in the wider community.

The School will endeavour to follow the guidance from the BECTA document:

"A school web site should take care to protect the identity of pupils: where a child's image appears, the name should not, and vice versa.
Parental permission should be obtained before using and images of pupils on the website.
If a school collects personal data in any form via its website this may be subject to data protection legislation; a clear and detailed privacy statement should be prominently displayed on the site stating how the information will be used.
Schools should also take care to protect intellectual property on their site and should not provide any information which could breach copyright law."

Disposal

Ruislip Gardens Primary School network uses central data storage for all information and User files.

Data is not stored on desktop or tower PCs. When these PCs are disposed of, the discs will be security-erased.

Staff laptops synchronise with the school network and so may store sensitive data on the hard disk. When laptops are disposed of, the disks will be securely erased or physically destroyed.

It is the responsibility of the user to ensure that copies of any personal files are obtained before the laptop is handed back to the school for disposal or reuse.

File servers will be disposed of via an organisation which can securely erase the disks, or else the disks will be physically destroyed.

Staff from External Agencies
Staff from external agencies, may be given access to the school network and to appropriate data held in it. Such persons must be identified (preferably in writing) in advance and must carry and wear an appropriate employee identification badge.

Access will only be given to those areas which are appropriate to the work of that person in school and will be controlled by network and application passwords. The person will be required to process this data only in accordance with their own terms of employment and will be forbidden from removing data from the system without authorisation from their employer and the Head teacher of the school.

Legal Responsibilities
Requirements
Ruislip Gardens Primary School conforms to the requirements of the Data Protection Act (1998) and the Freedom of Information Act (2000).

Storage of Data
The fifth principle of the 1998 Act states that "Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes." The guidance suggests that:

- Finance Data should be kept for 6 years or as laid down by Local Authority Financial Regulations.
- Pupil and Staff Data should be kept for 7 years, after which a school might not be required to provide exam results or references. In practice, core data archived by the SIMS system may be kept for longer than this, depending on the recommended configuration of the system.

Updates to this Policy
In the light of changes in the business, technology, legislation or relevant standards it may be necessary to update this policy from time to time. Notification to all staff will be made when updates are available.

Disciplinary and related action
Ruislip Gardens Primary School wishes to promote the highest standards in relation to good practice and security in the use of data. Consequently it expects and supports the integrity of its staff. In exceptional circumstances, where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

Password Policy
Access to the School Network and to data stored on it is controlled by a school password. Special database programs, such as the SIMS system, have separate access controls in addition to this.

User names and passwords must never be communicated to any other person, nor should any person log in to the network for another person. This could result in unauthorised access to information.

Network passwords must:

- be at least 6 characters in length.
- contain a mixture or letters and numbers.

- ideally contain at least one capital letter (passwords are case sensitive).

The network will force the user to choose a new password after 8 weeks.
Users cannot re-use previous passwords.

It is not good practice to use the same password for all applications, though it can be sensible to have a small number of passwords in use at any time.

Passwords must never be written down.

Phil Jones, Facilities Manager June 2012
Edited by Mr Jeans, ICT – Coordinator January 2013