Gilbert Scott Primary School
Data Protection/Information Security Policy

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

Gilbert Scott 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, Gilbert Scott 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 of destruction.

Gilbert Scott 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/Information Security Policy.

What is Information Security?

Information Security involves the protection of information and of the computer equipment and networks which hold and deliver that information. Although the protection of information is paramount, the IT systems on which that information is stored, transmitted and used must also be protected to the same high standard.

Why Is Information Security Important?

Head Teachers, as the "Data Controllers" under the Data Protection Act 1998 ('DPA'), are responsible for the safety and security of data held by that establishment. Schools hold some very confidential information about both staff and pupils. Whether this is hard copy or electronic on fixed or portable device or cloud storage, this must be kept secure and only accessed by the limited number of staff who need to see it.

Principle 7 of the DPA provides that 'appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data'.

What Personal Data Do We Use at Gilbert Scott?

Personal data is information which relates to an identifiable living individual that is processed as data. Processing means collecting, using, disclosing, retaining or disposing of information. This also includes education records including names of staff and pupils, dates of birth, addresses, national insurance numbers, school marks, medical information, school reports, SEN information and staff development reviews. This data may be electronic or in paper format.

Sensitive personal data relates to race, ethnicity, political opinions, religious beliefs, members of trade unions, physical or mental health, sexuality and criminal offences. There are greater legal restrictions on sensitive personal data.

Individual Responsibilities

Everyone has responsibility for the security of the IT systems that they use and the information that they hold.

We must all preserve the **Confidentiality** of information when required by:

- ensuring that only authorised people can gain access to confidential information by keeping it secure; and
- not disclosing confidential information to anyone who has no right to see it.
- Ensure sensitive data is shredded before disposal

We must all preserve the **Integrity** of information by:

- making sure that the information we record is correct; and
- making sure that we understand how any system should be used and be briefed on any updates or changes to it.

We all must maintain the **Availability** of information by:

- ensuring that equipment is protected from loss or damage;
- ensuring that backups for which we are responsible are taken at regular intervals; and
- not entrusting sensitive or confidential information to any system that does not offer an adequate level of protection.

Further information is available on the Information Commissioners' Office website (https://ico.org.uk/for-organisations/education/).

How Do We Keep Data Secure at Gilbert Scott?

We will ensure that data at Gilbert Scott is kept secure by:

- Making sure all computers, laptops and tablets require passwords in order to gain access to individual accounts.
- Staff should make sure that their passwords have been changed from the default password to keep data secure. Passwords for standard users should not be simple. They should include some numbers and or capitals. They must **never** be left blank or set to standard passwords like "password", "Password", or even "1234". These provide little or no security.
- Passwords should be changed regularly and not be written down. Staff should not share their passwords and ensure they are kept confidential. If there is any indication that anyone else knows their password, staff should immediately change their password.
- Passwords must not be stored as part of automatic logon sequences for machines, software or secure websites. Passwords for administrator accounts must be complex and consist of at least eight characters including a combination of capital letters, lower case letters and numbers. Ideally, at least one symbol should be included as well. In order to protect data on unattended machines being used by staff, there is a password-protected screensaver that automatically cuts in after 10 minutes.

How Portable Storage Devices will be used at Gilbert Scott

Portable Data Storage Devices can be used to store and transport data from one device to another, e.g. a memory stick. Most of these devices are small, light, portable and easy to use. These same qualities make them very easy to lose or to have stolen. Portable Data Storage Devices permit the removal of large amounts of data that may be confidential and is potentially at risk if it leaves the relative safety of a school network. If such a device is lost or stolen, the data on it may fall into the hands of someone who has no right to see it and could process such data unlawfully.

Under the Data Protection Act, data controllers (the Head Teacher) are required to undertake appropriate technical and organisational measures sufficient to prevent unauthorised or unlawful processing of any personal data held on any devices in their school/academy. The ICO has made it clear that encryption is expected and there could be a fine imposed on a school if it had to self-report a breach involving loss or theft of personal data on an unencrypted portable device.

The only portable data storage devices that will be used at Gilbert Scott are encrypted memory sticks provided to teachers, the School Business Manager and the Headship Team. These USB memory sticks, that may hold personal data, will be military-style encrypted, so you will need to enter a password to unscramble the data before use. This will prevent anyone else from reading the data if it is lost or stolen. No other memory sticks should be used in school. We encourage staff to use the storage area on the school server or the LGfL USO as a secure alternative to using pen drives.

Staff should avoid using very sensitive data from the school network and also staff should avoid taking paper copies of sensitive data offsite but, when this is absolutely necessary, staff should ensure they are kept safely.

How Cloud Storage will be used at Gilbert Scott

Cloud storage – such as Microsoft OneDrive, or Google Drive – is increasingly being used as an alternative to USB memory sticks. Cloud storage allows for large amounts of data to be uploaded and then downloaded to multiple devices.

Cloud storage can be used at Gilbert Scott, but the account must be secured with a password matching the instructions on page 3 of this policy. It is also expected that any information uploaded to Cloud storage is encrypted, as is necessary when carrying data via a USB memory stick.

Staff should avoid uploading very sensitive data to Cloud storage, unless it absolutely necessary.

Disposal of Redundant ICT Equipment

At Gilbert Scott we ensure any obsolete computer equipment have any hard drives wiped and taken out before being recycled with a reputable company where we receive a Waste Electrical and Electronic Equipment Regulations (WEEE) certificate to ensure they are disposed of securely and disposed in an environmentally friendly way. We ensure all residual data has been securely removed beforehand in line with Principle 7 of the Data Protection Act. This is completed by the school IT technicians in collaboration with the school Business Manager. These items will be taken off the school's asset plan and marked for disposal by the school Business Manager/IT technician.

Protecting Data from Accidental Loss

The school will ensure that confidential data is kept securely and understands their responsibility to guard against important information being lost accidentally. School based records for individual staff and pupils are kept locked in metal filing cabinets so they are protected from fire damage and water damage. Both the admin and curriculum networks have back-ups which are kept off-site securely to prevent data loss.

Reporting Security Incidents

A security incident is anything that could damage the security of your school network, supported laptops, mobile devices or information held on that system. Staff should be aware of the risks of inappropriate use of the IT systems and must report to the Headship Team any weakness in security (actual or potential) which they come across.

These are examples of security incidents:

- Attempts by someone else to obtain your password.
- Attempts by other people to use your computer whilst it is logged in under your name.
- The theft or loss of equipment - laptop, tablet, data disks or USB memory stick.
- The abnormal behaviour of a programme – this may be evidence by a "viral infection".

If you are uncertain, it is better to report the problem. If the incident is serious, users should also inform their department head or Head Teacher as soon as possible.

Physical Security

- Appropriate building security measures are in place
- Visitors to school are required to sign in and out, to wear identification badges whilst in school and be accompanied where necessary

Sharing Information

- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the school by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school who needs to know the information in order to do their work.
- The school will not disclose anything on pupils' records which would reasonably be likely to cause serious harm to their physical or mental health or that of anyone else, including anything which suggests that they are, or have been either the subject of or at risk of child abuse.
- A 'legal disclosure' is the release of personal information from the computer to someone who requires it to do their job within or for the school, provided that the purpose of that information has been registered.

- An `-illegal disclosure is the release of information to someone who does not need it, or has no right to it, or one which falls outside the school's registered purposes.

Access to personal Information

The school will comply fully with our duty to respond to any requests for access to personal information.

The school will make a charge of £10.00 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.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Any complaints which are not appropriate to be dealt with through the school's complaints policy can be dealt with by the Information Commissioner.

Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every two years. This policy will be agreed and ratified by the Governing Board.

Any enquiries in relation to this policy should be addressed to the Head Teacher, who will also act as the contact point for any Subject Access Requests.

Links to other policies

- Health & Safety
- Safeguarding & Child Protection
- Staff Code of Conduct
- Online Safety
- Equality

Date agreed - May 2017

Renewal – May 2019