The Stonehenge School Secure Data Handling Policy

Overview

Personal data

School staff have access to a wide range of personal data concerning children and families. Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by data protection legislation (General Data Protection Regulation 2016 and Data Protection Act 2018) as "Personal data that includes information relating to natural person who can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information". Examples of personal data include, but are not limited to; names, dates of birth, the name of their parents or guardian, address and contact numbers as well as legal information and curricular data. Sensitive information may also be held in accordance with our safeguarding policy.

The GDPR sets out seven key principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality (security)
7. Accountability

The Data Protection Act states that some types of personal information demand an even higher level of protection, these are known as special categories of personal data. The GDPR defines special category data as
:

- Personal data revealing racial or ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious or philosophical beliefs
- Personal data revealing trade union membership
- Genetic data
- Biometric data (where used for identification purposes)
- Data concerning health
- Data concerning a person's sex life and
- Data concerning a person's sexual orientation

The Data Protection Act applies equally to personal data recorded in electronic form or on paper.

Secure Handling

In accordance with principle of the GDPR personal data must be handled in a secure fashion.

The three questions below can be used to quickly assess whether information needs to treated securely, i.e.
1. Would disclosure / loss place anyone at risk?
2. Would disclosure / loss cause embarrassment to an individual or the school?
3. Would disclosure / loss have legal or financial implications?

If the answer to any of the above is “yes” then it will contain personal or commercially sensitive information and needs a level of protection. This document summarises how the school will protect personal data.

Principles

The following principles will be applied within the school:

- The amount of data held by the school should be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personally sensitive data held by the school will be securely stored and sent by secure means.

Securing and handling data held by the school:

Electronic data

ICT systems and MIS should be managed in such a way that protected files can be given permission levels, with protected files being hidden from unauthorised users. Access to data should be granted as required for the employee's role only.

Personal and sensitive data should 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). Auto-lock (WINDOWS+L) should be enabled when devices are left unattended.

Staff should not use memory sticks to store personal data and the transfer to memory sticks from school PC's is disabled. If data is required to be transferred to or from a memory stick (e.g. for Exam Board requirements) this should be undertaken by a member of the IT team. This data will then be encrypted and sent securely.

Any files stored on the network that requires a high level of protection should either be password protected or stored in an area that only the relevant individual has access to.

The Stonehenge School requires users to have strong passwords, which are changed regularly. User passwords must never be shared.

Storage media is stored in a secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school and Children's Centre equipment (this includes computers and portable storage media (iron keys issued to all staff). Private equipment must not be used for the storage of personal data.

Staff Owned Devices

- Staff must not use their own devices to take images of clients
- Only school equipment may be used and images must be deleted as soon as they are no longer required, saved securely on school systems and deleted in accordance with the retention policy.
- Staff should not save the personal numbers of students to their devices
- Pass-codes or PINs must be set on personal devices to aid security; and where possible encryption applied to the device
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements
- Users must log out of school systems, programmes and applications when they are not in use
- The device must have the latest updates applied
- Passwords must not be saved, for example to the browser history
- Users must not download data locally to the device (e.g email attachments)

When personal data is stored on any mobile device or removable media:

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

The Stonehenge School does not recommend the use of "Cloud Based Storage Systems" (for example DropBox, Google Apps and Google Docs)

Data transfer should be through secure websites e.g. (S2S, PerspectiveLite). If this is not available then the file must be minimally password protected or preferably encrypted before sending via email, the password must be sent by other means and on no account included in the same email. A record of the email should be kept, to identify when and to whom the email was sent, (e.g. by copying and pasting the email into a Word document).

When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by a technician using a recognised tool, e.g. McAfee Shredder.

The school's wireless network (WiFi) will be secure at all times.

Data Disposal

In accordance with the 5th principle of the DPA (Data shall not be kept for longer than is necessary) the Stonehenge School will comply with the legal 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 for data.

Paper Records

The Stonehenge School will endeavours to keep the number of paper records it holds to a minimum. Any sensitive paper records should be kept in a lockable location. Paper records can be taken off site; these must also be stored in a portable lockable box. The Stonehenge School will operate a "Clean Desk" policy where no sensitive records should be left attended.

Compliance

Auditing

The school must be aware of all the sensitive data it holds, be it electronic or paper.
A register will be maintained detailing the types of sensitive data held, where and by whom, and will be added to as and when new data is generated.
Regular audits will take place; the frequency of the audits will be determined by the school's Data Protection Officer. The audits will assess security measures are already in place and whether or not they are the most appropriate and cost effective available.

This register will be sent to relevant staff each year to allow colleagues to revise the list of types of data that they hold and manage.

The audit will be managed by the Data Protection Officer and staff designated by them.

Training

All staff need to be trained on electronic secure data handling and need to be reminded of their responsibilities, as per this policy. This will be the responsibility of the Headteacher in conjunction with the Data Protection Officer.

Training normally takes the form of an induction, as well as annual training as part of Safeguarding. Any relevant updates involving the emergence of new technology will be given as they arise.

Staff in the school sign an Acceptable Use Policy acknowledging that they have attended data protection training and understand their responsibilities.

Data Breach and reporting incidents

Logs will be kept by the Data Protection Officer of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use police.

All significant data protection incidents will be reported by the Data Protection Officer to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Policy Review

This policy will be reviewed by the Data Protection Officer on an annual basis.
If you would like to discuss anything in this data handling policy please contact our our **data protection officer via e-mail on** . dpo@stonehenge.wilts.sch.uk