Feb 2018 then updated Oct 18

STANBRIDGE LOWER SCHOOL

GENERAL DATA PROTECTION REGULATIONS POLICY

February 2018

1. AIMS

1.1 Our school aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the General Data Protection Regulations (GDPR) 2018. This policy also complies with regulation 5 of the Education (Pupil Information)(England) Regulations 2005 which gives parents the right of access to their child's educational record.

2. CONTENTS

3. DEFINITIONS

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as:

	• Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording or holding data
Data subject	The person whose personal data is held or processed
Data controller (SCHOOL)	A person or organisation that determines the purposes for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. THE DATA CONTROLLER

4.1 Our school processes personal information relating to pupils, staff and visitors, and, therefore, is a data controller.

4.2 The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

4.3 The school has two Data Protection Leads; Miss R Godwin and Mrs N Coupland who are responsible for ensuring the school's procedures and processes comply with GDPR.

5. DATA PROTECTION PRINCIPLES

5.1 We follow these data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully

- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection 2018.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data

6. ROLES AND RESPONISBILITIES

6.1 The governing body has overall responsibility for ensuring that the school complies with its obligations under the General Data Protection Regulations 2018. Governors monitor compliance with GDPR in 6 monthly cycles.
6.2 Day-to-day responsibilities rests with the Head Teacher or the Senior Teacher in the Head Teacher's absence. The Head Teacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.
6.3 Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.
6.4 The General Data Protection Regulations lead person in school is Miss R Godwin and Mrs N Coupland. The lead person Miss R Godwin ensures a full GDPR audit is completed annually by an external company.

7. PRIVACY/SHARING OF DATA/FAIR PROCESSING NOTICE

7.1 Pupils and parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education. All details are contained in our Pupil Privacy Notices available to read on the school website at www.stanbridge.beds.sch.uk

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected. All details are contained in our Staff Privacy Notices available to read on the school website at www.stanbridge.beds.sch.uk
Any staff member wishing to see a copy of information about them that the school holds should contact the Head Teacher in writing using the Subject Access Requests forms available on the school website at www.stanbridge.beds.sch.uk

8. DATA SECURITY

8.1 Data security procedures detailing what staff can/can't store on laptops, ipads, notebooks, and any other mobile device including discs, USBs and external hard drives etc. are described in detail in this section.
8.2 All electronic data is categorised as public, restricted or protected.

Restricted Information Containing Sensitive Personal Data	Protected Information	Public Information
Personal information related to pupils and staff contained in all Management Information Systems eg Integris, Classroom Monitor etc. Examples of these are SEN information, reports, academic results, medical information etc.	School routines, schedules and management information	Website and promotional materials, display material around school, school dates etc
Should only be accessed by the Head Teacher and staff with designated passwords. Teaching/Office Staff: should only transfer restricted data using an encrypted USB, or Anycomms. All transfer of paper records should be signed for	Can be accessed by all staff on the shared curriculum area. This is password protected.	Accessed by all via websites

8.3 The procedures to ensure all members of the school staff know their access rights, data protection responsibilities and safeguarding responsibilities when using ICT are detailed in the Staff Acceptable User Policy.

8.4 All mobile storage devices are vulnerable to theft or loss and there are confidentiality risks when using these away from school. Staff should not store any restricted information/data on mobile storage devices.

8.5 The Head Teacher will keep a log of all mobile devices used and who they are allocated to. Staff should not use their own mobile devices in school eg laptops, ipads, external drives. All mobile devices should be owned and issued by school.

8.6 We prevent unauthorised physical access to premises, equipment and interference to personal data. We

- Restrict access to a "need to know" basis only. Access levels to management information systems are restricted by usernames and passwords and only designated members of staff allowed access to complete their work.
- Implement appropriate entry controls; doors, locks, alarms, security lighting
- Have effective visitor procedures eg signing in, name badges, escorting round building if appropriate.
- Locate equipment housing sensitive data in separate rooms protected by additional controls.
- Have a "clear desk" expectation of all staff during and at the end of the day
- All ICT equipment including mobile devices are username and password protected using strong passwords. Have a 10 second lockdown/clearscreen on all internal computers.
- Promptly collect documents from printers and photocopiers and ensure these are switched off outside business hours
- All mobile devices should be kept securely overnight and when not in use.

8.8 We prevent the exploitation of technical vulnerabilities by

- Using the latest versions of operating systems, web browsers, applications ensuring these are updated regularly. Our ICT technicians manage this for us.
- We have a well configured firewall as this is recognised as the first line of defence against external attack and can help prevent data breaches by blocking malware and hacking attempts.

9. DATA BREACHES

9.1 All breaches of security including cyber attack, loss or theft of mobile storage devices should be reported directly to the Head Teacher who will investigate this and implement a recovery/assessment plan.

9.2 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

9.3 The full Data Breach Procedure can be found at the end of this policy in Appendix A and it can also be found on our website at www.stanbridge.beds.sch.uk

Example

Personal data breaches can include:

- Loss or theft of personal data and/or equipment on which data is stored
- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.
- Hacking attack
- Cyber attack
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Flawed data destruction procedures

9.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

9.4 Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

9.5 In the event of a security incident or data breach the following procedure will be followed:

- ***Containment & Recovery***
  Lead person to investigate; who needs to be informed; act to contain breach by recover losses and/or limit damage
- ***Assessment of ongoing risk***
  Establish what data involved; events; individuals affected; nature of harm and possible wider consequences

- **Notification of breach**
  Within 72 hours Identify whether need to report to ICO; inform individuals; if reporting to ICO, include details of what happened and steps taken to mitigate/minimise impact
- **Evaluation & Response**
  Identify weak areas in data security and implement measures to tighten security, monitor and improve

All staff should escalate a security incident to the appropriate person immediately so they can determine whether a breach has occurred.

9.6 When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO; if it's unlikely then we won't report it and our reasons documented.

9.7 When reporting a breach we will provide

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; andthe categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

9.8 If any individual is affected by the breach when it is likely to result in a high risk to their rights and freedoms they will be notified of this without undue delay. The individual will be offered advice and support to help protect themselves from the effects of the breach.

9.9 We will provide the affected individual with

- A description in clear and plain language, the nature of the personal data breach and, at least:
- the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and

- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

9.10 We document all breaches even if they don't have to be reported.

9.11 For a more detailed Data Breach procedure. Please see the attached Data Breach Management Procedure.

10. STORAGE OF RECORDS

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use. All access keys are kept in a secure location.
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must gain permission from the Head Teacher and then sign the electronic or paper records in and out from the school office using the Transfer of Records Receipt. This is overseen by office staff who then complete the Transfer of Sensitive Data Log. Office staff must ensure the receipt and log are signed when records are returned into the school building.
- Staff, pupils or governors SHOULD NOT store PROTECTED AND SENSITIVE information on their personal devices IPHONES – NUMBERS, RESULTS ETC

11. PASSWORD SECURITY

11.1 Electronic Records are password protected. Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, USBs and other electronic devices.

11.2 Staff and pupils are reminded to change their passwords at regular intervals

12. DISPOSAL OF RECORDS

12.1 Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred or incinerate paper-based records, and override electronic files. We may at times also use an outside company to safely dispose of electronic records.

12.2 We routinely "weed" electronic data and paper based records that are no longer relevant or out of date.

13. TRAINING

13.1 Our staff and governors are provided with data protection training as part of their induction process.

13.2 All staff and governors are briefed on their GDPR responsibilities including the creation, use, maintenance, privacy of PII and eventual destruction of records. They are briefed on security as set down in this policy. GDPR responsibilities are refreshed with staff yearly and this forms part of our annual training.

13.3 Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

14. MONITORING AND REVIEW PROCEDURES

14.1 The Governing Body is responsible for monitoring and reviewing this policy, and the Head Teacher has the responsibility for ensuring the procedures outlined in the policy are adhered to, as delegated by the Governing Body.

14.2 Miss R Godwin and Mrs N Coupland checks that the school complies with this policy by, among other things, reviewing school records 6 monthly.

14.3 The governing body will nominate a member to monitor the implementation of this policy during a monitoring visit every 6 months.

14.4 The Head Teacher will organize for an annual GDPR check by an external agency.

14.5 The school's policy will be reviewed when:

- 2 years have elapsed.
- There has been a significant change in staff, pupils or the law.
- The school wishes to review the policy.

.

15. LINKS WITH OTHER POLICIES

- This data protection policy and privacy notice is linked to the freedom of information publication scheme.
- E Safety Policy
- Staff Acceptable User Agreement
- Pupil Acceptable User Agreement
- Governor Code of Conduct
- Child Protection Policy

R J Godwin
Head Teacher
October 2018

This policy was ratified by the full governing body.

Date of Meeting: ……………………………………….

Signed ……………………………………………………………. Chair of Governors.

Appendix A

Stanbridge Lower School
Data Breach Management Procedure

Policy Statement

As an organisation which processes personal data, every care is taken to protect personal data and to avoid a data protection breach. This policy outlines the measures our school takes against unauthorised or unlawful processing or disclosure and against accidental loss, destruction of or damage to personal data.

In the event of data being lost or shared inappropriately, our school will take appropriate action to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by **our school** and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

This Data Breach Procedure document forms part of the school's Data Protection Policy and all staff are made aware of these procedures through induction, supervision and ongoing training.

Purpose

It is a regulatory requirement under GDPR for our school to have consistent and effective governance and control arrangements to protect the personal data that we hold. This Data Breach Procedure sets out the course of action to be followed by all staff in the event of a real or potential data protection breach.

Definition of data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In summary, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Personal data breaches can include:

- Loss or theft of personal data and/or equipment on which data is stored
- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission;
- loss of availability of personal data
- hacking attack
- cyber attack
- equipment failure
- human error
- unforeseen circumstances such as a fire or flood
- flawed data destruction procedures

Aims of Data Breach Management Procedures policy

The aim of this policy is to ensure a standardised and consistent approach is followed when responding to data breaches to enable us to:

- report data breaches without delay to the Head Teacher and/or Data Protection Lead
- Identify incidents of data breaches quickly and investigate them properly and in a timely manner
- record and document all incidents and report them to the Senior Leadership Team (SLT), Governors and the Data Protection Lead(s)/DPO
- asses the severity and impact of the data breach to determine whether it is necessary to inform the Data Subject(s) and ICO according to the GDPR guidance
- take action which is proportionate, consistent and transparent to prevent further damage
- regularly monitor and review all data breach incidents and potential situations that may lead to a data breach to identify improvements in policies, procedures and control mechanisms to remove or mitigate risk of further repetition

Reporting a data breach

As soon as any member of staff, parent or governor discovers or receives a report of a data breach, they must inform the Head Teacher and/or the Data Protection Lead as soon as possible and without delay. If the breach occurs or is discovered outside normal school working hours, then notification should begin as soon as is practicable.

A verbal or emailed report can be submitted to the Head Teacher and/or Data Protection Lead in the first instance and should include accurate details of the incident.

An initial assessment of the data breach by the Head Teacher and/or Data Protection Lead will include completion of the **Data Breach Incident Report Form** to ascertain as much information as possible about the incident in order to fully assess the impact of the data breach and determine actions required.

Managing a data breach

Step 1: Containment and Recovery

1. The Head Teacher and/or Data Protection Lead will ascertain the severity of the breach, whether any personal data is involved and whether the breach is still occurring.

2. If the breach is still occurring, the Head Teacher and/or Data Protection Lead will establish what steps need to be taken immediately to minimise the effect of the breach and contain the breach from further data loss (e.g. alert the school's IT Technical support, restricting access to systems or close down a system etc).

3. The Head Teacher and/or Data Protection Lead will consider and implement appropriate steps required to recover any data loss where possible and limit damage caused (e.g. use of backups to restore data; changing passwords etc.)

4. The Head Teacher and/or Data Protection Lead will inform the Chair of Governors if the severity and likely impact of the breach deems it necessary to inform the ICO of the breach. At the same time, depending on the nature of the breach, the Head Teacher and/or Data Protection Lead may seek expert or legal advice and/or the Police if it is believed that illegal activity has occurred or likely to occur.

5. Where a significant breach has occurred, the Head Teacher and/or Data Protection Lead will inform the ICO within 72 hours of the discovery of the breach (see Notifications below).

6. The decision taken as to the reasons why a data breach is either reported or not reported is documented by the Data Protection Lead.

7. All the key actions and decisions are fully documented and logged in our Data Security Breach Log.

Step 2: Assessment of Risk

Further actions may be needed beyond immediate containment of the data breach. To help the school determine the next course of action, an assessment of the risks associated with the breach is undertaken to identify whether any potential adverse consequences for individuals are likely to occur and the seriousness of these consequences.

The Head Teacher and/or Data Protection Lead will consider the points arising from the following questions:

1. What type and volume of data is involved?
2. How sensitive is the data? Could the data breach lead to distress, financial or even physical harm?
3. What events have led to the data breach? What has happened to the data?

4. Has the data been unofficially disclosed, lost or stolen? Were preventions in place to prevent access/misuse? (e.g. encryption)
5. How many individuals are affected by the data breach?
6. Who are the individuals whose data has been compromised?
7. What could the data tell a third party about the individual? Could it be misused regardless of what has happened to the data
8. What actual/potential harm could come to those individuals? E.g. physical safety; emotional wellbeing; reputation; finances; identity theft; one or more of these and other private aspects to their life
9. Are there wider consequences to consider?
10. Are there others that might advise on risks/courses of action (such as banks if individual's bank details have been affected by the breach)?

Step 3: Notification of breaches

If the severity and likely impact of the breach warrants notifying the ICO, then we will notify the ICO within 24 hours of becoming aware of the essential facts of the breach (through the ICO's online portal at https://report.ico.org.uk/security-breach/).

This notification will include at least:

- our school name and contact details
- the date and time of the breach (or an estimate)
- the date and time we discovered it
- basic information about the type of breach
- basic information about the personal data concerned.

As we undertake a full investigation of the details of the breach, **within 3 days of the initial notification**, we will further provide the ICO with full details of the incident, the number of individuals affected and its possible effect on them, the measures taken to mitigate those effects, and information about our notification to the individuals affected.

There may be instances when the nature of the breach and the individual(s) affected may necessitate notifying third parties such as regulatory bodies, agencies, professional bodies as part of the initial containment.

If the breach is likely to adversely affect the personal data or privacy of our pupils, parents/carers, staff and/or governors, we will notify them of the breach without unnecessary delay if we cannot demonstrate that the data was encrypted (or made unintelligible by a similar security measure). We will inform them of:

- the estimated date of the breach
- a summary of the incident
- the nature and content of the personal data
- the likely effect on the individual(s)
- any measures we have taken to address the breach
- how those affected can mitigate any possible adverse impact

Step 4: Evaluation and response

When the school's response to a data breach has reached a conclusion, the Head Teacher and/or Data Protection Lead will undertake a full review of both the causes of the breach and the effectiveness of the response. The full review is reported to SLT and the Governing Board for information and discussion as soon as possible after the data breach has been identified.

If through the review, systematic or ongoing problems associated with weaknesses in internal processes or security measures have been identified as a cause of the data breach, then appropriate action plans will be drafted, actioned and monitored to rectify any issues and implement recommendations for improvements. The Governing Board will be party to discussions regarding action plans and be able to monitor progress against the actions appropriately.

If a breach warrants a disciplinary investigation, legal advice will be sought through Human resources channels.

Implementation of these procedures
The Head Teacher and/or Data Protection Lead will ensure that staff are aware of these procedures for reporting and managing data breaches. Data Protection training for all staff is mandatory, including new employees and all staff will undertake refresher training annually.

If staff have any queries or questions relating to these procedures, they should discuss this with the Head Teacher and/or Data Protection Lead.

Complaints about our Data Breach Management procedures
If an individual or Data Subject affected by a data breach believes that a data breach has not been dealt with properly, a complaint should be made to the school through our normal complaints procedure. If following the conclusion of the complaints procedure within the school, the individual or Data Subject is still dissatisfied, then a complaint can be made directly to the Information Commissioner’s Office (ICO) at https://ico.org.uk/concerns .