Charlton Kings Infants' School

Personal Data Handling Policy

Governor Committee Responsible:	Finance and Operations	Governor Lead:	Alan Waller Alan.Waller@ckis.org.uk
Status	Non-Statutory	Review Cycle	Bi-Annual
Last Review	1.06.2019	Next Review Date	June 2021

Designation	Name	Date	Signature
Chair of Governors	Henning Schmidt	12.06.19	
Head Teacher	Katie James	12.06.19	

INTRODUCTION

Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office for the school and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

Policy Statements

The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Privacy Notice section below)

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils/students, members of staff and parents/carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular/academic data eg class lists, pupil/student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Responsibilities

The school's Senior Information Risk Officer (SIRO) is the Headteacher. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs)

The school will identify Information Asset Owners (IAOs): The Data Manager for student and assessment data and the Business Manager for Staff data. The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents/Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents/carers of all pupils/students of the data they collect, process and hold on the pupils/students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents/carers through the school websites and via electronic mail/letter. Parents/carers of young people who are new to the school will be provided with the privacy notice through the website, electronic mail/letter.

Training & Awareness

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings/briefings/Inset
- Day to day support and guidance from Information Asset Owners

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

The following risks have been identified and categorised (see Appendix 1 for Government Guidelines on Protective Marking):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Like-lihood	Overall risk level (low, medium, high)	Action(s) to minimise risk
1	Student personal contact data	Data Manager	3	Low	Low	Password protocol/tiered and restricted access
2	Staff personal contact data	Business Manager	3	Low	Low	Password protocol/tiered and restricted access
3	Staff data eg absence/PDA	Business Manager	2	Low	Low	Password protocol/tiered and restricted access
4	Student assessment data	Data Manager	2	Low	Low	Password protocol/tiered and restricted access

Impact Levels and protective marking

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students/pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "**When you have finished with it, this document should be added to one of the secure storage facilities for confidential information for destruction; these are located in the data office and Reception**".

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly ie a minimum of 8 characters and containing at least one upper case character, one number and one 'other' character eg -, /, & etc. User passwords must never be shared. Personal data may only be accessed on machines that are securely password protected.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media. Private equipment (ie owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data/device must be encrypted and password protected,
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Stroud High School has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups – see SHS Technical Security and Back-up Policy.

Stroud High School has clear policy and procedures for the use of "Cloud Based Storage Systems" (for example Dropbox, Google apps and Google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data services providers to protect the data.

As a Data Controller, the Stroud High School is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site with the exception of school trips where the material is the responsibility of the trip leader.

Stroud High School recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place (see Freedom of Information Act 2000 Policy) to deal with Subject Access Requests ie a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably use secure remote access to school systems;

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required. This retention/destruction of personal data and confidential school information will comply with the Retention Guidelines document provided for schools by the Information and Records Management Society.

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 or be disposed of through an approved third party.

Documents for destruction by an approved third party will be added to one of the secure storage facilities for confidential information for destruction. These storage facilities will be emptied by either the Site Manager or Deputy Site Manager and disposed of through that approved third party; certificates of secure destruction will be retained by the Business Manager.

It is recognized that the Site Manager and Deputy Site Manager will have contact with confidential personal/organisational material etc in the course of their duties. It is the Site Manager's responsibility to ensure that the emptying of secure disposal storage is restricted to the him/herself and the Deputy Site Manager with the understanding that contents of such files must be kept confidential; Site Manager and Deputy Site Manager job descriptions reflect this requirement.

Audit Logging/Reporting/Incident Handling

Audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example. All incidents will be logged with the Network Manager

The school has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

This is a flowchart from SWfGL detailed in the e-Safety and Security Policy

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Appendix 1 - Use of technologies and Protective Marking

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	May apply in Stroud High School eg some meeting minutes
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	Will not apply in schools

Most student/pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The following from the SWGfL provides a useful guide:

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publicly accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil/student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil/student record available in this way.

Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via “dashboards” of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Date of Policy: October 2016 Next Review: October 2019

Reviewed by Resources Committee