HALL GREEN SCHOOL

DATA PROTECTION POLICY
(Updated: April 2018)

Adopted:	28 March 2018
Next Review:	28 March 2020
Governing Committee:	Senior Management Team
Responsibility:	Mr D Adams – Headteacher
	Mr A Simson – Deputy Headteacher
	Mr M Hosfield – Deputy Headteacher
	Mrs P Evans – Assistant Headteacher
	Mr R Slattery – Assistant Headteacher

DATA PROTECTION GUIDANCE AND INFORMATION FOR STAFF

Under the GDPR, the data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

What is personal data?

According to Article 2(a) of the GDPR, "personal data! is defined as "any information relating to an identified or identifiable natural person ("data subject!); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". As a consequence, any information containing two or more of the following would be classified as personal data:

- Religion
- Ethnicity
- FSM status
- Name
- DOB
- Photographs of the data subject
- Address
- Parental contact information
- UPN (Unique Pupil Number)
- Medical information – e.g. disabilities
- Form group information/class information
- Assessment information
- Anything else that could cause embarrassment to a child or parent or bring the school's good name into disrepute.

Separate consent is obtained for the use of biometric data, which is classified as "sensitive personal data". Biometric data is used by Chartwell, our catering company, to provide an alternative method of identifying pupils and staff when purchasing items.

Individual rights

The GDPR provides the following rights for individuals (data subjects):

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

For further information, please visit https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights. Privacy notices are available for parents/carers, pupils, staff and children currently looked after (CLA) at http://www.hallgreen.bham.sch.uk/policies.

Article 6(1)(c) provides a lawful basis for processing where "processing is necessary for compliance with a legal obligation to which the controller is subject". In circumstances such as the census, this applies. In all other cases where data processed would not be required legally, the home/school agreement constitutes consent to process this data.

Demonstrating compliance: Organisational protocols

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles". As an organisation, Hall Green School ensure that in order to fully comply with GDPR, the following processes will be followed:

- Personal data regarding staff and pupils will be destroyed or disposed of once the relevant retention period has expired.
- Privacy policies are in place for staff, pupils and parents/carers.
- Contracts will be in place with all data processors, stipulating the legal requirement for them to adhere to the GDPR principles.
- We will ensure comprehensive whole-school staff training, internal audits of processing activities and reviews of internal HR policies.
- We will maintain relevant documentation on processing activities.
- We have a designated data protection officer (DPO) - Mr Ryan Slattery (Assistant Headteacher).
- We will implement measures that meet the principles of data protection by design and data protection by default. Where possible, data minimisation, pseudonymisation and transparency are employed.

- We allow individuals to monitor processing.

- We will create, apply and improve security features on an ongoing basis.

- We use data protection impact assessments. This means that before any proposed data-processing agreement is finalised, an internal assessment must take place where the DPO and any other relevant parties discuss details and log the outcome and decision.

Demonstrating compliance: Staff protocols

As an individual member of staff, you have a personal responsibility to act in a professional way to maintain the integrity of data and engage in all of these organisational protocols implemented by Hall Green School as they relate to our obligation to comply with GDPR and uphold the rights of any data subject(s). For all members of staff, the following personal directives must also be adhered to:

When storing or working with data

- Only store pupil data on school equipment, e.g. network drives (staff area, staff shared area etc.). Only school-issued encrypted USB devices are permitted. **Any member of staff using a personal USB device as opposed to a school-issued USB device may be subject to disciplinary procedures.**

- Staff must not routinely take pupil data off-site if it contains sensitive information that could either identify a pupil or cause embarrassment if the data was lost/seen by another individual. In cases where staff feel this is unavoidable, please see the SIRO. Marking of books or pupil work should not be considered a risk, provided extraneous pupil data is not present.

- Staff are responsible for destroying their own data once it is **no longer required.** This should be immediately after the "event" or at the end of the academic year if it is required for a longer period of time. Pupil coursework can be destroyed once certification is obtained, but may be retained for longer if staff feel this is necessary. If this is the case, the individual retaining it is personally responsible for secure storage and destruction before the pupil in question is twenty-five years of age (nine years after the pupil leaves school).

- Diaries that contain notes from meetings etc. that identify pupils or staff should be stored securely when not in use.

- When socialising do not discuss any individuals from work as you are never fully aware of who is listening.

- Never send personal information regarding pupils or staff via pupils.

- Staff must take every precaution to ensure they do not display potentially personal/sensitive data on smartboards or in visible documents. SIMS/ClassCharts/e-mail should not have pupil or staff details "broadcasting" to pupils, if those details could cause undue distress, alarm or embarrassment. It is perfectly reasonable to have the register document open in SIMS, the seating plan (without personal data) on ClassCharts or any other information with generally "known" information.

- In cases where information regarding pupils, parents or staff would be sent via email, you should consider whether the content could significantly compromise the data subject if read by another

party. For example, details regarding bereavement, health, special needs or safeguarding concerns should be password protected within a word document.

- If using social media, you are advised to use a screen name, do not accept students as 'friends', and do not discuss work-related personal data.

When communicating within and outside of Hall Green School

- You must take personal responsibility for checking email addresses/groups/contact details if you are sharing personal or sensitive data. **Any data breaches attributed to entering incorrect details are the responsibility of the individual.**

- When communicating with any individual, staff must always use professional and appropriate language. Remember that all communications could be the subject of a Freedom of Information request, and thus become a public document if the data subject chooses.

- In cases where an email contains personal data which should be retained on record, staff must write a note or complete a report in SIMS and then delete the email.

- It is advised that you delete/empty email trash every 3 months. In an investigation records of all kinds are called for, and staff are personally responsible for the ongoing maintenance of their school email accounts

- All electronic communications with pupils and parents must be through school email addresses, texting services and the official School Twitter account. When contacting pupils, it is only permitted to email their school email address, not a pupil's personal email address.

- Staff must ensure adequate and appropriate security measures are taken when accessing email/pupil data/work-related content from personal devices such as mobile phones, tablets, laptops and personal computers. Accounts should always require a password to be entered, and should not be automatically saved (auto-login).

- When printing and distributing data subject information, this should only be relevant for the purpose, should not contain extraneous information and the number printed should not exceed the number required.

- Do not leave computers or electronic devices unlocked and unattended in a classroom, if they contain personal data. Keyboards must be locked and screens must not be showing personal data. If an offence is committed by a third-party whilst a device is logged in, the person whose login is used is also responsible even if they do not commit the offence.

- Do not take or store photos of pupils on personal devices.

- If a third-party wishes to use images/footage of our pupils, they must obtain consent themselves. Our consent record only applies to our own use (Twitter/website/promotional material etc.). It DOES NOT mean third-parties can assume consent. They MUST obtain separate written permission (usually through their own consent form)

- You must check the updated permissions list before using pupil photographs

- Records of assessment or meetings must be shredded once the work is no longer needed.

- ROA reports must be spell-checked and proof-read to minimise data inaccuracy.

- Trip documentation should be destroyed once you are confident that the trip occurred without incident. If an incident has occurred documents must be submitted to Mr J Sheard and will be kept for 25 years. If unsure, you must speak to Mr J Sheard or Mr R Slattery immediately upon your return.

- Information on walls in offices/classrooms where parents may be taken for meetings must be covered up or removed before the meeting is held.

Staff should be aware that data breaches resulting from a deliberate or grossly negligent failure to adhere to the personal responsibilities under the school data protection protocol could result in disciplinary procedures. In any case when the act of negligence is significant enough to warrant the involvement of the Information Commissioner or potential legal proceedings, Hall Green School will fully support any external enquiry.

Information Loss Process

In cases where a member of staff has become aware that a potential information loss has occurred, they must report the loss immediately to the SIRO (Senior Information Risk Owner – Mr R Slattery). Regardless of circumstances, reporting must occur within **72 hours.**

The reporting process will involve:

- discussing the nature of the data
- the potential implications of the loss
- the potential need to inform parents, the police or the Information Commissioner
- determining if disciplinary action is required due to negligence.