Hall Orchard CE Primary School Data Policy
Incorporating General Data Protection Regulation and Freedom of Information
May 2020 to May 2022

Scope and Purpose of this Policy

- This policy applies to all staff and governors in the handling of data on behalf of Hall Orchard CE Primary School.
- This policy will be reviewed every two years by the Head teacher or person/s appointed by the Head teacher

Roles & Responsibilities

The school has a Data Protection Lead (Officer) and a Freedom of Information Lead appointed by the Head teacher. He/she is responsible for:

- Reviewing this policy for presentation to Governors;
- Taking due regard for government requirements and guidelines regarding the use of data;
- Policy implementation and monitoring including staff training;
- Ensuring that any Freedom of Information and Subject Access Requests are responded to appropriately;
- Together with the Head Teacher, responding appropriately to any data breaches in the school to ensure that the impact of such is minimised whilst maintaining an open and honest manner in informing the appropriate stakeholders of the breach.
- All staff who manage or come into contact with data will sign to say they have received training on this policy and that they understand their responsibilities as laid out.

Other staff have particular responsibilities for data handling and controls, it must be emphasised however that all staff must have due regard to data policies in carrying out their day-today work.

The school complies with its duties under the GDPR (2018). The school is registered with the Information Commissioner's Office as a data controller.

Staff and governors should have due regard to the 6 principles of the Act.

Data should be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;
2. 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;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. 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;
5. 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
6. 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."

Data Processing Procedures

- The school only holds the data which it deems to be necessary to: facilitate and enhance teaching and learning and pastoral care; ensure the safety of students and staff; and carry out appropriate administration.
- An information audit map will be carried out and reviewed annually. Regular ongoing updates will take place throughout any academic period. Staff across the school will have the ability to contribute to this ongoing process. Where staff are responsible for being the designated person in managing any updates this will be clearly explained in both training and recorded in procedures and policies such as this policy.
- This is known as the Information Asset Register (IAR)

- **A Data Protection Impact Assessment (DPIA) - sometimes referred to as a Privacy Impact Assessment (PIA) will be carried out as required but particularly when planning a new initiative that may involve 'high risk' data processing. Staff across the school may be involved at different levels in delivering these PIA's.**

- Privacy notices are made available to all staff and parents and to pupils in years 5 and 6, to inform them that the school holds data on them and who the school may share this information with.
- These notices are updated periodically.
- All data that is gathered, whether relating to pupils, staff or other stakeholders, is kept as up-to-date and as accurate as possible.
- A data collection sheet/s may be issued to parents/carers for checking on a rolling program if required.
- Wherever possible the information is collected electronically via parental and staff direct input. For example Parent Lite.
- When the school is informed of a change to personal data, computer and papers records are updated as soon as practical.
- All staff and governors have a duty to ensure that data they hold is kept secure. Specific information regarding that can be found in the **Acceptable Use Policy for Data (Appendix 1).**
- The school follows national guidelines regarding data retention. Paper copies of personal data will be shredded when no longer needed and electronic copies deleted. Hard drives are securely wiped when being disposed of.
- Educational records, including but not limited to SEND records, are stored until the pupil is 25, and then securely disposed of.
- Employee personnel records will be held for the length of employment plus 7 years, before being securely disposed of, with the exception of documents relating to child protection or accidents at work which may be held for longer periods.
- With regards to subject access requests (SAR's), whereby any pupil or member of staff may request access to his/her personal data, the school complies with the GDPR and follows guidance from the Information Commissioner's Office.
- Access requests will be dealt with within 28 days of a written request being received. In the case of pupils making such a request, they may normally be given a copy of their data directly, unless the school feels that the pupil does not understand the nature of the request in which case this will be discussed with parents/carers, or the data is outside the provision of the GDPR.
- Note: if the volume of material requested is considered large or exceptionally time consuming to collate an additional period of up to two more months is available. BUT the school will communicate that they will be using this time or a proportion of it and why as early as possible but within 30 days and indicate when they will complete the work.
- Data may be shared with the Local Authority, DfE and other schools to allow the school to fulfil its statutory obligations, or to enable the transfer of information when a student leaves or joins the school. Details of who we share data and why are on the relevant Privacy Notice

The Freedom of Information Act

- Hall Orchard CE Primary School is committed to the Freedom of Information Act (2000) and to the principles of accountability and general right of access to information, subject to legal exemptions.
- Under the Act, any person has a legal right to ask for access to information held by the school. They are entitled to be told whether the school holds the information, and to receive a copy, subject to certain exemptions. Requests under the Freedom of Information Act are different to subject access requests (see section above).
- The school routinely makes information available to the public as defined in the Information Commissioner's Office model publication scheme. Much of this information can be found on the school website, or is otherwise available by contacting the school. Requests for other information will be dealt with in accordance with statutory guidance. While the Act assumes openness, it recognises that certain information is sensitive. There are exemptions to protect this information.
- Our process for responses to Freedom of Information requests is outlined in our **Acceptable Use Procedure for Data.** We have a duty to respond to all requests within 20 working days (excluding school holidays).
- Where information is subject to an absolute or qualified exemption under the Act, we will inform the person making the request of this, after invoking the public interest test procedures as appropriate. Any complaint made following this will be handled as per the school's complaints procedure.
- The Data Protection Lead and Freedom of Information Lead must be made aware of all Freedom of Information requests. A register of these will be kept.

Use of CCTV

- Under the Protection of Freedoms Act 2012 the processing of personal data captured by CCTV systems (including images identifying individuals) is governed by the GDPR and the Information Commissioner's Office (ICO) has issued a code of practice on compliance with legal obligations under that set of regulations.
- The school uses a CCTV system to monitor the rear gates for the security of the site. The CCTV system is maintained by the Business Manager. The school's standard CCTV cameras record visual images only and do not record sound. The schools system records for a period of not less than 7 days and not more than 9 days with successive days being overwritten.
- The school has notified the Information Commissioner's Office of the purpose for which the images are used. All operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are trained in their responsibilities under the CCTV Code of Practice.
- Access to recorded images is restricted to staff that need to have access in order to achieve the purpose of using the equipment. All access to the medium on which the images are recorded is documented. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images.
- Recorded images will be stored in a way that ensures the integrity of the image and in a way that allows specific times and dates to be identified. No access is made of live images.
- Recorded images can only be viewed by approved staff. The recorded images are viewed only when there is suspected criminal activity, or activity which could be harmful to pupils and staff, and not for routine monitoring of pupils, staff or visitors.
- The school reserves the right to use images captured on CCTV where there is activity that the school cannot be expected to ignore such as criminal activity, potential gross misconduct, or behaviour which puts others at risk.
- The retention of recordings for evidential purposes will be authorised by the Headteacher or a member of staff to whom this authorisation has been delegated to by the Headteacher.
- Disclosure of the recorded images to third parties can only be authorised the Headteacher or a member of staff to whom this authorisation has been delegated to by the Headteacher.
- Disclosure will only be granted:
    - If its release is fair to the individuals concerned.
    - If there is an overriding legal obligation (eg information access rights).
    - If it is consistent with the purpose for which the system was established.

- All requests for access or for disclosure are recorded. If access or disclosure is denied, the reason is documented

Note: Disclosure may be authorised to law enforcement agencies, even if a system was not established to prevent or detect crime, if withholding it would prejudice the prevention or detection of crime.

Subject Access Requests

- Individuals whose images are recorded have a right to view images of themselves and, unless they agree otherwise, to be provided with a copy of the images. If the school receives a request, this will be handled as per the above directions.
- As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access, it will be deemed personal data and its disclosure is unlikely. Refusal to disclose images may also be appropriate where their release is likely to cause substantial and unwarranted damage to the individual, or to prevent automated decisions from being taken in relation to that individual.

Notes: this policy is subject to change and development as the General Data Protection Regulation and associated legislation and schedules and articles are better understood across the sector.

Further Information

Hall Orchard CE Primary School
Church Street
Barrow upon Soar
Loughborough
Leicestershire
LE12 8HP
Tel 01509 412 188
e-mail: DPLO@hall-orchard.leics.sch.uk

Our data controller registration number provided by the Information Commissioner's Office is: Z654746X

APPENDIX 1
Hall Orchard CE Primary School
Acceptable Use Policy for Data
May 2020 May 2022

All staff and governors should be aware of this agreement, and agree to follow it as a condition of their employment or involvement with the school. Failure to do so may result in disciplinary action.

It is vital that the school fulfil its obligations under the General Data Protection Regulation (2018) and Freedom of Information Act (2000). All staff are given training on this, however this Acceptable Use Policy has been put together to ensure that all staff are aware of and follow specific rules.

Data to which this AUP applies

- Personal data is defined as data with two or more personal identifiers (e.g. name and address, name and date of birth). *Please see Appendix 3 below*
- Sensitive data is any data that could harm, discomfort or embarrass an individual if it were to become public or be made available to an unauthorised individual. For example SEN, racial or medical data, bank details, phone numbers.
- This AUP also applies to other confidential data such as performance management documents.

Security of paper-based data

- Staff are responsible for ensuring that data issued to them remains secure. On site this means keeping data away from being easily accessible by unauthorised personnel e.g. pupils, parents and other visitors to site.
- If taking data off site, paperwork should be stored securely at all times. You should remain with the data when in transit, and store it in a secure area e.g. a locked cupboard.
- Data should never be taken outside of the EU.
- Particularly sensitive data, e.g. SEND or medical records, payroll details etc, should never be removed from the school site and remain in a secure area e.g. locked cupboard, filing cabinet or office at all times.
- All paper based records containing data should be securely shredded when no longer of use. You should not keep records beyond this time, unless advised otherwise (e.g. child protection records must be kept for longer).
- Staff are reminded that a 'clear desk' policy should be adhered to at all times.
- Hard copy data that identifies a data subject could form the basis of a data breach
- Material should not be left 'out' in teaching spaces where the public including parents could view or remove the material.

Security of electronic data

- Passwords to access computers, and laptops will be a **minimum of 10 digits** and must include the following formats,
    - numerical,
    - letters both lower and upper case
    - and characters
- These passwords will be changed each month, unless a security breach or other similar concern is identified.
- Passwords are not to be shared with any other members of staff
- Support members of staff including cover supervisors **must sign into SIMS or other required class software** using their own passwords
- You must ensure that you lock or log out your computer when leaving it unattended, even for a short period of time.
- All staff are reminded that all computers and laptops must be switched off at the end of each day
- Data left visible on screens would form the basis for a breach

- When you leave the classroom for breaks, dinner and similar periods screens must be screen locked ALT,CONTROL,DELETE – Lock
- Computers left on with just screens switched off would provide access to data covered under the legislation
- You are responsible for activity that takes places using your credentials, which can be monitored.
- No USB's are used in school
- Staff will be required to make use of Office One Drive instead or SharePoint for collaboration work
- Teachers and support staff will confirm that their assigned IPad has a suitable pin code or password set to access it.
- If here is no pin code or password the teacher or other member of staff will be responsible for ensuring this is completed by returning the IPad to the IT technician.
- No data should be stored in any format or location that allows pupil access.
- For the avoidance of doubt material to accessed outside of schools should where possible be stored and accessed via Office One Drive this includes
    - Email
    - Any documents that provide information on data subjects and by their nature come under the GDPR legislation
- Data that comes under GDPR should not be stored on school laptops
- All school laptops must be encrypted and it the responsibility of the laptop user to ensure they have confirmed with the schools IT technician that encryption has been installed
- All laptop users must ensure the school laptop they use is made available as requested by the school ICT technician.
- If a laptop is lost this must be reported to the GDPR lead and the headteacher within 24 hours.

Photographic/Digital Images

- Photos and videos of students **must only** be taken using school owned devices.
- Any exception to this can only be authorised by the Headteacher or a deputy approved by the Headteacher in writing.
- The placing of photos on websites and social media must be approved by the Headteacher or a member of staff to whom this approval has been delegated to by the Headteacher.
- All files containing images of pupils must be deleted in line with the School's Retention Policy, this will normally be within one year of its original intended purpose or where other legislation does not expressly provide legal reason to retain within one year of the pupil leaving the school.
- If you use your mobile device(s) to access school email you must make sure that they are protected with a suitably strong and robust password or pass-code login.
- If your device is lost or stolen you must inform the Data Protection Lead (Officer) or the Headteacher within 24 hours of the loss.
- You must ensure your personal devices are logged off and not kept logged in after accessing your email.
- When you leave the school, be aware that your accounts for the network, email and other systems will be disabled when your contract ends.

Release of data to others

- Staff may share information with each other regarding students as necessary in the performance of their duties, as long as this sharing of information is in the best interests of the students. The only exception to this is where a manager has explicitly stated that information is not to be shared.
- When sharing data with another organisation e.g. another school, you should check the legitimacy of the potential recipient.
- Wherever possible, school-to-school student data transfers will be made by the data admin staff using the secure B2B and S2S systems. If you are unsure you should consult a Senior Leader, and always check before sending data out of the country.
- Staff with access to data regarding other staff, such as contracts and pay scales, should ensure they have been granted permission to access this data by the Head or Deputy Head.

Email

- Staff will use the school provided email account for all email related to your work for the school. This system is managed by the school with appropriate controls and security measures in place.
- For the avoidance of doubt **Under no circumstances will staff use their personal email to conduct school business.**
- The only exception for this will be if the Headteacher has given written approval.

Data Breaches

- The school takes any data breach very seriously. Should you become aware of any such breach or the potential for one, you should inform a Senior Leader immediately.
- Under GDPR data controllers (the school is a data controller under the legislation) have a legal obligation to inform the Information Commissioners Office of data breaches within prescribed time periods.
- These are very short periods depending on the breach conditions but are measured in a small number of days at the longest.

Freedom of Information and Subject Access Requests

- Any member of staff or the Governing Body may receive a subject access request for personal data, or a request for information under the Freedom of Information Act. Such requests will be made in writing or by email.
- If you receive such a request, you should inform the Data Protection and Freedom of Information Officer immediately, or in his/her absence the Headteacher. The school has a legal duty to respond to requests within a time limit, so it is important that you pass on the request in a timely manner.
- The Data Protection Lead and Freedom of Information Lead or Headteacher will manage the appropriate response and if appropriate inform you of the outcome.
- **Staff should be aware that, in fulfilling requests, the school may be required to disclose the contents of emails or hard copy communications.**
- It is therefore vital that staff remain professional in all correspondence.
- It is an offence to wilfully conceal, damage or destroy information in order to avoid responding to an enquiry, so it is important that no records that are the subject of an enquiry are amended or destroyed

Appendix 2
Additional Information

What is the difference between a data controller and a data processor?
Data protection law draws a distinction between a 'data controller' and a 'data processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. It is the data controller that must exercise control over the processing and carry data protection responsibility for it. The new GDPR is a European wide directive.

"Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or are to be processed. This includes senior leadership to include governors at school

"Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. This should include LEAMIS, the LA payroll and pension's provider, any other government body or similar who process data where the school is the data controller. The LA may also be acting as a data controller when is manages personal data for children, parents and staff. This also includes organisations providing services to the school such as

- SIMS
- Schoolcomms
- Parent Mail
- CPOMS (Safeguarding)
- Edukeyapp (SEND)
- Fronter (VLE)
- apps.eskimo (Foundation Profiles app)
- IRIS Connect (videoing)

"Processing", in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

a) Organisation, adaptation or alteration of the information or data,
b) Retrieval, consultation or use of the information or data,
c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) Alignment, combination, blocking, erasure or destruction of the information or data

The definition of processing can be useful in determining the sort of activities an organisation can engage in and what decisions it can take within its role as a data processor.

The definition of 'processing' suggests that a data processor's activities must be limited to the more 'technical' aspects of an operation, such as data storage, retrieval or erasure.

Activities such as interpretation, the exercise of professional judgement or significant decision-making in relation to personal data must be carried out by a data controller. This is not a hard and fast distinction and some aspects of 'processing', for example 'holding' personal data, could be common to the controller and the processor.

Processing required by law
Where personal data are processed only for purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller, i.e. SIMS data for children or personal data for payroll purposes.

This means that where an organisation is required by law to process personal data, it must retain data controller responsibility for the processing. It cannot negate its responsibility by 'handing over' responsibility for the processing to another data controller or data processor. Although it could use either type of organisation to carry out certain aspects of the processing for it, overall responsibility remains with the organisation with the statutory responsibility to carry out the processing.

With the above explained it is clear the school as an organisation is a data controller and cannot transfer its responsibility to another body though another body may carry out some of the functions, i.e. data storage were the LA acts as a secure back up provider in case of total loss at the school.

Why is it important to distinguish between data controllers and data processors?

If all parties are working well together to make sure that compliance issues such as giving subject access or keeping personal data secure are addressed, then the question of data protection responsibility may seem academic. However, the distinction between a data controller and data processor can have significant real-world consequences. For example, if there is **a data breach** it is essential for both the organisations involved and the ICO to be able to determine where responsibility lies.

This can be difficult, and there is evidence of confusion on the part of some organisations as to their respective roles and therefore their data protection responsibilities. It is important that the various organisations involved in a data processing activity establish their roles and responsibilities at an early stage, particularly before the processing commences. This will help to ensure that there are no gaps in organisations' responsibilities – such gaps could result in subject access requests going unanswered, for example.

http://wdsolicitors.ie/data-protection-exam-script-personal-data/

Was the Examination Paper "Personal Data" within the meaning of the Acts and/or the Directive?

"Personal data" is defined within the Acts as follows:

"*[D]ata relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller*."

The court noted that if the result of an examination is capable of being personal data, then it might be argued that the raw material by which that result is arrived at, either itself, or in conjunction with the examiner's comments, is also personal data.

https://www.irishtimes.com/news/crime-and-law/failed-exam-candidate-gets-right-to-written-paper-in-ecj-ruling-1.3334566