Data Protection & Portable Devices Policy

P

1. Rationale

1.1 This policy sets out how all staff and governors at Light Hall School ('the school') ensure that personal information[i] is dealt with correctly and securely and in accordance with relevant Data Protection law ('the Law'), including the General Data Protection Regulations (GDPR), as well as related UK Data Protection legislation.

1.2 Portable device procedures have been developed by the Head Teacher and Senior Leaders. It is based on guidance from the Information Commissioner Office (ICO) to ensure the protection and the safe keeping of personal data, and to comply with the requirements of the Date Protection Act. It also complies with the requirements of the IT Acceptable Use Policy, the School Code of Conduct and the E-Safety policy.

1.3 It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

1.4 In addition, this policy complies with our funding agreement and articles of association.

1.5 The school processes personal data relating to parent, pupils, staff, governors, visitors and others and therefore is a data controller.

1.6 The school is registered with the ICO and has paid its data protection fee to the ICO as legally required.

1.7 The data protection officer (DPO) is responsible for overseeing the implementation of this policy, and monitoring compliance with data protection law. The school's data protection service is provided by the Information and Governance Team at the Local Authority who act as the DPO.

1.8 A deliberate breach of this Policy will be treated as a disciplinary matter.

2. Data Protection Law

2.1 The GDPR provides a framework for how organisations use personal information. It protects and enforces the privacy of personal information whilst also allowing for the lawful and appropriate use of this type of information about pupils, staff, parents and others who have contact with the School.

2.2 The Law applies to many types of organisation processing personal information, including Schools. It covers all personal information regardless of its format or the way it is collected, used, recorded, updated, stored and destroyed.

2.3 Personal information relates to an individual who can be identified by that information or along with other information likely to come into a person's possession. The School acknowledges that the definition also covers opinions about an individual, information regarding the intentions of the school towards them, and more sensitive 'Special Categories'[ii] of information.

2.4 The GDPR is underpinned by a set of six straightforward principles; the School is committed to following these principles as set out in this policy. These are set out in paragraphs 3-9.

3 Processed Lawfully, Fairly and Transparently

3.1 The School will inform pupils, staff, parents and any other person why they need their personal information, how it will be used, with whom it may be shared and anything else required. This will be done via clear and easy to understand statements on forms and Fair Processing Notice documents issued when collecting information or as soon as possible afterwards; they will also be published on the School website where relevant.

3.2 For the majority of personal information the School's lawful basis for processing it is it is necessary for compliance with a legal obligation. Where this is not the case, consent to use personal information will be sought from individuals.

3.3 Where necessary, the School will conduct Privacy Impact Assessments to ensure the processing of information by the school does not pose a risk to the rights and freedoms of pupils, staff, parents and any other data subjects.

4 Collected for Specified, Explicit and Legitimate Purposes

4.1 Personal information collected and held for the purposes we have stated will not be used for any other purpose without first informing those individuals whose information it is.
4.2 In accordance with UK law the School is registered as a Data Controller with the Information Commissioner's Office and will renew this annually.
4.3 In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's record retention schedule.

5 Adequate, Relevant and Necessary

5.1 The School will only collect and store personal information that is sufficient for the purpose we have stated and will not ask for more information than is necessary.
5.2 The School will regularly review its forms and will check personal information already held for missing, irrelevant or seemingly excessive information.

6 Accuracy

6.1 Information held by the School will be as accurate and up to date as is reasonably possible and steps will be taken to regularly check the accuracy of personal information held; an example is the annual data collection form issued to all parents to check details are up-to-date.
6.2 If a pupil, member of staff, a parent or any other person informs the School of a change of circumstances or an error in their personal information it will be reviewed and updated as soon as is practicable.

7 Retention of Information

7.1 The School will not keep personal information for longer than is necessary for the stated purpose(s). In order to ensure this, all information held and/or created by the School or held on its behalf will be retained according to timescales set out in the Retention Schedule created by the school (see appendix one).
7.2 The School will ensure that all personal information deleted or physically destroyed is done in a secure and confidential way.

8 Access

8.1 The School acknowledges that the Law gives specific rights[iii] to any person whose details are processed by the School, and will ensure these rights can be exercised where relevant.
8.2 These rights include the right to access information held about them.[iv] The School will ensure clear procedures are in place to allow for this and will supply the information sought within the required timescale of one calendar month from date of written request.
8.3 A written request from parents/carers in respect of their own child will be processed as requests made on behalf of the child and the copy will be supplied to the parents/carers
8.4 Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.
8.5 The right to access information held about them applies equally to staff and any other individuals for whom the school holds information.
8.6 Any third party information (information about someone other than the requesting individual) found will generally be removed or redacted unless third party permission to disclose is provided or it is reasonable in all circumstances to disclose it.
8.7 In addition to the right to make an access request (see above), and to receive information when we are collecting their data about how we use and process it , individuals also have the right to:

- Withdraw their consent to processing at any time

- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- Be notified of a data breach (in certain circumstances)
- Make a complaint to the ICO

9 Appropriate Security

9.1 To prevent unauthorised or unlawful processing and to protect against accidental loss, destruction or damage to personal information, the School will ensure adequate security measures are in place to safeguard all personal information whether held in paper files, on a computer system, laptop/tablet or on portable media storage devices.

9.2 In order to prevent the loss of any personal data Light Hall School operates a mandatory procedure, whereby, any school information can only be transported on a Light Hall encrypted memory stick or laptop issued by the IT team.

9.3 Encrypted portable devices should be used for transporting data ONLY not as a permanent means of storage. The data should be securely deleted from the device once it has been transferred to the school network.

9.4 The use of non-encrypted portable devices (e.g.) memory sticks, memory cards, portable hard drives is not allowed.

9.5 Light Hall (memory stick) devices:

- Have to be pre-registered by IT using SOPHOS to allow the device access to the school network
- Are password protected and allocated to a specific user.
- Are encrypted using WINDOWS BITLOCKER software.

9.6 Non-school (memory stick) devices that may also be using WINDOWS BITLOCKER software will not be able to access the school network as they will not be recognised as an authorised device.

9.7 All other school devices:

- Memory cards for cameras, video, audio recorders Etc. are not allowed direct access to the network
- On request IT will download any data from the school device; then upload and back it up to the network.

9.8 THE EXAM OFFICER routinely uses unencrypted USB's with school laptops for the saving of exam work, the laptops are NOT connected to the school network. All data saved on these devices is then encrypted by IT before sending to the exam board.

9.9 THE MUSIC DEPARTMENT routinely use unencrypted USB's with the MAC DESKTOPS for accessing music software, the MAC's are NOT connected to the school network; all data is saved locally to the machines.

9.10 Paper records and portable devices are locked away when not in use and are only accessed by those authorised to see the information held on them. Personal information held electronically is kept securely, is protected by passwords, and is only accessed by those authorised to see the information held.

9.11 Where it is necessary to store or transport personal information on a portable device such as a laptop/tablet or other storage device the relevant equipment or portable media will always be encrypted.

9.12 The School will ensure that staff are aware of the additional precautions they should take when taking personal information, in any format, outside of school for training, meetings or to work from home, such as only taking what is needed, protecting it in transit, never leaving it unattended and storing it securely.

9.13 Particular care will be taken by all staff when sending personal information via emails, faxes and letters, etc. to use secure methods where necessary and to confirm addresses/numbers beforehand.

9.14 The School will undertake a regular review of measures in place to protect personal information taking into consideration developments in technology and ensuring staff receive up to date training and guidance.

10 Remote Network Access

10.1 The School uses remote access software using either RDS (remote desktop server) or SOPHOS VPN (Virtual Private Network) to enable staff to work remotely, all users are preregistered remote for access by IT.

10.2 All school functions are accessible via remote working

10.3 The remote access software prevents localised printing of documents.

10.4 Remote working should ideally be done:

- only from the staff members home and using their home Wi-Fi
- from a password protected device
- used where the screen cannot be easily observed by others
- not done from mobile devices using external Wi-Fi hotspots

10.5 The software at time of this report cannot prevent SCREEN SHOTING or COPY & PASTE facilities

10.6 Remote access software and functions are routinely reviewed and amended continually.

11 Using Data Processors

11.1 The School will ensure that any third parties who process personal information on the School's behalf will do so under strict written instruction that is binding on the third party, who will also have adequate safeguards in place to protect the information.

11.2 Records of checks of adequate security and the written instruction will be maintained by the School for reference and regular review.

12 Transfers Outside of Europe

12.1 Data Protection law applies to all member states within the EU and the UK. The School is unlikely to transfer any personal information outside of the UK and Europe, however, if this is necessary, checks will be made to ensure an adequate level of protection for that information and consent will be sought from those affected if necessary.

13 School Specific Issues

13.1 **Consent** - the School will seek consent/parental consent to use certain types of personal information where appropriate. Examples of when the School will seek consent include using photographs or recordings of children in school for school projects or for display; using photographs of children, staff and parents in school publications such as newsletters; using photographs of children, staff and parents in external publications such as a local newspaper; using photographs/recordings of children, staff and parents to be on any web page or social media site.
When collecting consent the School will provide a clear explanation of the use of the information and will ask for a positive written indication of consent for each different use. Consent will not be inferred from a non-response to a communication, for example from a parent's failure to return or respond to a letter.

13.2 **CCTV** - the School utilises CCTV for security and safety purposes. CCTV footage will feature personal information; therefore the School ensures access to the footage and equipment is restricted and makes sure that pupils, staff, parents and visitors to School premises are aware that CCTV is in use by displaying clear signage in and around School premises. We use CCTV in various locations around the school site to ensure it remains safe. We adhere to the ICO's code of practice for the use of CCTV

13.3 **Public Displays -** If there is a display of pupils' work to be shown at a public venue, (other than the school premises), parents will be informed and unless they have consent to publish fuller information, the School will only include the minimum of pupil identifiable information, for example "by John, year 1".

13.4 **School Plays -** Data Protection law does not prevent parents/guardians from capturing their child's performance on camera or video as these instances would be for personal/family use only and therefore Data Protection law does not apply. However, the policy of Light Hall School is that parents/guardians are NOT permitted to capture public performances on camera or video

14 Complaints

14.1 Complaints will be dealt with in accordance with the School's complaints policy. Complaints relating to information handling may also be made to the Information Commissioner's Office (the statutory authority).

15 Contacts

15.1 If you have any enquires in relation to this policy, please contact the Head Teacher's P.A. who will also act as the contact point for any access requests.

16 Review

16.1 This policy will be reviewed and updated as necessary to reflect best practice or amendments made to Data Protection law and annually by the leadership group and governors

[i] Inclusive of more sensitive personal information known as 'Special Categories' under the General Data Protection Regulations

[ii] This includes more sensitive information and includes information about a person's race, ethnic origin, political opinion, religious and philosophical beliefs, trade union membership, genetics and biometrics, their health, sex life and sexual orientation.

[iii] Under GDPR these are the right to be informed; the right of access; the right to rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; rights in relation to automated decision making and profiling

[iv] There are a few exceptions to this rule, but most individuals will be able to have a copy of the information held on them