

# Holly Park School Data Security Policy

## 1 Aims

1.1 The objectives of this Policy, which is intended for all school staff, including governors, who use or support the school's ICT systems or data, are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

## 1.2 **Links with the UN Rights of the Child**

### **Article 13**

Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.

### **Article 17**

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

## 2 Definitions

- 2.1 **Information**- covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.
- 2.2 **Personal Data** - Any data which can be used to identify a living person. This includes names, birthday and anniversary dates, addresses, telephone numbers, fax numbers, email addresses and so on. It applies only to that data which is held, or intended to be held, on computers ('equipment operating automatically in response to instructions given for that purpose'), or held in a 'relevant filing system'. This includes paper filing systems.
- 2.3 **Strong Password** – Password which is 8 characters minimum length, contains upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain dictionary words, the owner's date of birth or car registration number.
- 2.4 **Encryption** – Process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

## 3 Responsibilities

- 3.1 The Headteacher (Mrs A Pelham) is the school's Data Controller

- 3.2 The School shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act.
- 3.3 Users of the school's ICT systems and data must comply with the requirements of the Acceptable Use Policy (AUP) and ICT Security Policy.
- 3.4 The School's Leadership Group shall review this document at least annually.
- 3.5 Users shall be responsible for notifying the Headteacher of any suspected or actual breach of ICT security.
- 3.6 The Headteacher shall inform both the ICO and the Local Authority if there are any losses of personal data
- 3.7 Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990, Copyright, Designs and Patents Act 1988 and the Telecommunications Act 1984.
- 3.8 Users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.
- 3.9 Adequate procedures must be established in respect of the ICT security implications of personnel changes.
- 3.10 No personal data shall be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, external hard disks, memory sticks and Personal Digital Assistants (PDAs) & other removable media.
- 3.11 The school will make parents aware of a Privacy Notice. The School are the Data Controller for the purposes of the Data Protection Act. We collect information from Parents and may receive information from previous schools. We hold this personal data to -
- support teaching and learning;
  - monitor and report on progress;
  - provide appropriate pastoral care, and
  - assess how well the school is doing.
- We make parents aware of this through an information pack when they enter the school, once a year in 'Meet The Teacher' packs and on our school website.
- 3.12 Remote access to information and personal data shall only be provided through an encrypted link.
- 3.13 Users shall not publish spreadsheets, databases or other documents containing personal data on externally accessible web sites including the London MLE unless these documents are encrypted.

#### **4 Physical Security**

- 4.1 As far as practicable, only authorised persons should be admitted to rooms that contain servers or provide access to data.
- 4.2 Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.
- 4.3 All school owned ICT equipment and software should be recorded and an inventory maintained.
- .

- 4.4 Uninterruptible Power Supply (UPS) units are recommended for servers and network cabinets.
- 4.5 **Do not** leave sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer.
- 4.6 **Do not** give out sensitive information unless the recipient is authorised to receive it.
- 4.7 **Do not** send sensitive/personal information via e-mail or post without suitable security measures being applied.
- 4.8 Ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.
- 4.9 All sensitive data should be cleared from desks and other surfaces over night and stored in a locked cupboard. This includes assessment data, dinner registers and pupil or family personal information

## **5 System Security**

- 5.1 Users **should not** make, distribute or use unlicensed software or data.
- 5.2 Users **should not** make or send threatening, offensive or harassing messages.
- 5.3 Users **should not** create, possess or distribute obscene material.
- 5.4 Users must ensure they have authorisation for private use of the school's computer facilities.
- 5.5 Passwords should be memorised. If passwords must be written down, they should be kept in a secure location.
- 5.6 Passwords **should not** be revealed to unauthorised persons.
- 5.7 Passwords **should not** be obvious or guessable.
- 5.8 Passwords should be changed if it is affected by a suspected or actual breach of security, e.g. when a password may be known by an unauthorised person.
- 5.9 Regular backups of data, in accordance with the recommended backup strategy, must be maintained.
- 5.10 Security copies should be regularly tested to ensure they enable data restoration in the event of system failure.
- 5.11 Security copies should be clearly marked and stored in a fireproof location and/or off site.

## **6 Virus Protection**

- 6.1 The school should ensure current and up to date anti-virus software is applied to all school ICT systems.
- 6.2 Laptop users should ensure they update their virus protection regularly.
- 6.3 Any suspected or actual virus infection must be reported immediately to the ICT Team and that computer shall not be reconnected to the school network until the infection is removed.

## **7 Disposal of Equipment**

- 7.1 The School shall ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.
- 7.2 It is important to ensure that any software remaining on a PC being relinquished for reuse is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- 7.3 The School shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

## **8 Monitoring and Review**


- 8.1 It is the responsibility of the Governing Body to monitor the effective deployment of this policy. This responsibility has been delegated to the Staffing and Pupil Welfare Committee.
- 8.2 This policy will be reviewed on an annual basis.

## **Document Control**

### **Revision History**

Version	Revision Date	Revised By	Revision
1.0	Autumn 2013	Ann Pelham	Updated
1.1	September 2014	Govs S&PW	Updated in light of safeguarding advice
1.2	September 2015	Govs S&PW	Updated
1.3	September 2017	Govs S&PW	Updated
1.4	September 2018	Govs S&PW	Updated
1.5	September 2019	Govs S&PW	Updated
1.6	Summer 2020	Govs S&PW	Updated
1.7	Summer 2021	Govs S&PW	Updated
1.8	Summer 2022	Govs S&PW	Updated

### **Signed by**

	Name	Signature	Date
Headteacher	Ann Pelham		19/7/22
Chair of Governors	Clare Hegarty		19/7/22

## Distribution

Shared with
<ul style="list-style-type: none"><li>• Staff via school server</li><li>• Staff via September Inset annually</li><li>• Staff via reading and signing Acceptable Use form</li><li>• Governors via committee meetings</li></ul>



Date for next review
Summer 2023

## **Data Security Acceptable Use Agreement Form**

### **This agreement covers the use of digital technologies**

This Acceptable Use Policy is intended to ensure:

- that staff will be responsible users and stay safe while using the internet and other communications technologies including email and social media.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school provides staff email, staff laptops, pupil laptops, class cameras, teacher encrypted memory sticks, class desk tops and school iPads to enhance staff work and enhance learning opportunities for pupils. We expect staff to agree to be responsible users.

### **Agreement**

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where appropriate, educate the children in my care in the safe use of ICT and embed online safety in my work with children.

- I will use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body
- I will not reveal my passwords to anyone to anyone except restricted authorised staff. I will not attempt to use anyone else's password.
- I will not allow unauthorized individuals to access email, internet, intranet, network, or other school/LA systems.
- I will ensure that all sensitive or confidential documents and data are saved, accessed and deleted in accordance with the school's GDPR data security and confidentiality protocols. All such data should be held on the shared drive, Google Drive, an encrypted memory stick or laptop provided by the school. Reception laptops are encrypted for the EYFS profiles to be held on them
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use approved, secure email systems for school business
- I will only use the approved school e-mail for communication with parents if necessary – e.g PTA business, trips, governors etc
- I will password protect any personal ipads or iphones that I access my school e-mail from and ensure that the e-mail also has password protection.
- I will not browse, download or send material that could be considered offensive to colleagues
- I will not download any software or resources from the Internet that can compromise the network or are not adequately licensed
- I will not connect a computer, laptop, memory stick or other device (including USB flashdrive) to the network/internet that does not have an up to date anti-virus software:  
External media must not be used in school unless verified as safe by the ICT team. Anti-virus and firewall must not be disabled. Encryption must not be bypassed.
- I will not bring in from home any other laptop or memory stick to use other than that given to me by the school

- I will not try to install or attempt to install programmes onto any device nor will I try to alter computer settings.
- I will not allow children access to my school laptop or e-mail
- I will not use chat or social networking during directed hours. I will not run personal chat/network programs in the background whilst in school.
- I will not use camera phones for taking images of pupils. I will only store images of pupils or staff at home with permission of the school.
- I will ensure that my mobile phone is stored away during lesson time in the classroom
- I will communicate with others online or via e-mail in a professional manner, not using aggressive or inappropriate language.
- I will use the school's learning platform in accordance with school and London grid for learning advice
- I will ensure that any private social networking sites/blogs that I create or actively contribute to are not confused with my professional role. I will ensure that my security settings are set to high.
- I will ensure that any confidential data that I wish to transport electronically from one place to another is protected by encryption and that I follow school data security protocols when using such data in any location
- I understand that data protection policy requires that information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching
- I understand that all Internet, e-mail and network usage can be logged and this information could be made available to the leadership team or governors on request
- I will immediately report any illegal, inappropriate or harmful material or incident to the appropriate person. This includes accidental access.
- I understand that there are computer rules for pupils and an acceptable use agreement for pupils. I will be aware of these and implement these.
- I will report immediately any damage or faults involving equipment or software.
- I understand that the rules set out in this agreement also apply to school ICT systems off site
- I understand that failure to comply with this agreement could lead to disciplinary action. This could include a warning, a suspension or police involvement.

### **User Signature**

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent safeguarding, data protection and online safety policies.

I agree to abide by all the points above.

Signature ..... Date

Full Name ..... (printed)

### **Authorised Signature (Head Teacher / Deputy)**

I approve this user.

Signature ..... Date

Full Name ..... (printed)



## **HOLLY PARK**

### **Pupil Acceptable Use Policy**

**All pupils must follow the rules in this policy when using school computers.**

**Pupils that do not follow these rules may find:**

- **They are not allowed to use the computers**
- **They can only use computers if they are more closely watched**

**Staff will show pupils how to use the computers.**

<b>Computer Rules</b>	
<b>1</b>	I will only use polite language when using computers
<b>2</b>	I must not write anything that might upset someone
<b>3</b>	I know that my teacher will regularly check what I have done on the school computers
<b>4</b>	I must not tell anyone my name, where I live or my telephone number over the internet
<b>5</b>	I must not tell any usernames or passwords to anyone except my parents
<b>6</b>	I must log off after I have finished with my computer
<b>7</b>	I must not use the computers in any way that stops other people using them
<b>8</b>	I will report any websites that make me feel uncomfortable to the teacher
<b>9</b>	I will tell my teacher if I receive any messages that make me feel uncomfortable
<b>10</b>	I will not try to harm any equipment or the work of another person on a computer
<b>11</b>	If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils

-----  
**Please return this slip**

### **Pupil Acceptable Use Policy**

**I agree to follow the school rules when using the school computers. I will use computers sensibly and follow the rules explained by my teacher**

**I agree to report anyone not using computers sensibly to my teacher**

**I also agree to tell my teacher if I see websites that make me feel unhappy or uncomfortable**

**If I do not follow the rules, I understand that this may mean I might not be able to use the computers**

**Pupil Name** \_\_\_\_\_

**Parent/Carer Name** \_\_\_\_\_ **Parent/Carer Signature** \_\_\_\_\_