ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

THIS DOCUMENT IS a statement of the aims, principles and procedures for the retention of data for Elms Farm Primary School.
IT WAS DEVELOPED in 2020 through a process of consultation with governors.
IT WAS APPROVED by the governing body in September 2020.
REVIEWED: March 2022, Sep 2023

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the School to achieve this, including to: -

- protect against potential breaches of confidentiality;
- ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- increase awareness and understanding at the School of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

INTRODUCTION

Information Security can be defined as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction.

Staff are referred to the School's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found in the policy folder in Staff Share/ Sharepoint.

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to, laptops, tablets, digital cameras, memory sticks and smartphones.

1.0 DATA PROTECTION

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

This policy applies to all members of staff, including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

2.0 GENERAL PRINCIPLES

All data stored on our IT Systems are to be classified appropriately (including, but not limited to, personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the School's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with the Head Teacher the appropriate security arrangements for the type of information they access in the course of their work.

All data stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by the school's ICT Technician or by such third party/parties as Head Teacher may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with Head Teacher unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to the Head Teacher who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

3.0 PHYSICAL SECURITY & PROCEDURES

3.1 Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

3.2 Available storage rooms, locked cabinets, and other storage systems with locks shall be used to store paper records when not in use. If you do not feel you have the appropriate and/or sufficient storage available to you, you must inform the Head Teacher as soon as possible.

3.3 Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

3.4 The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Head Teacher as soon as possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the School to ensure physical security of the building and storage systems:

- The School carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.
- The School has a system to minimise the risk of unauthorised people from entering the school premises.
- The School close the school gates during certain hours to prevent unauthorised access to the building. An alarm system is set nightly.
- CCTV Cameras are in use at the School and monitored by the Site Manager
- Visitors should be required to sign in at the reception, and never be left alone in areas where they could have access to confidential information.

4.0 COMPUTERS & IT EQUIPMENT

The IT Technician, in collaboration with the Head Teacher, shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the School's security requirements;

b) ensuring that IT Security standards within the School are effectively implemented and regularly reviewed, working in consultation with the School's management, and reporting the outcome of such reviews to the School's management;
c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the IT Technician, in collaboration with the Head Teacher, shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy;
b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relate to personal data, informing the Data Protection Officer];
e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
f) monitoring all IT security within the School and taking all necessary action to implement this policy and any changes made to this policy in the future; and
g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

5.0 **RESPONSIBILITIES: MEMBERS OF STAFF**

51. All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

5.2 Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

5.3 You must immediately inform the Head Teacher of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Data Breach Policy.

5.4 Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the IT Technician immediately. You are not permitted to install any software of your own without the approval of the Head Teacher Any software belonging to you must be approved by the Head Teacher and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

5.5 Prior to installation of any software onto the IT Systems, you must obtain written permission by the the Head Teacher. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

5.6 Prior to any usage of physical media (e.g. USB memory sticks or disks of any kind) for transferring files, you must make sure to have the physical media virus-scanned. Approval from the Head Teacher must be obtained prior to transferring of files using cloud storage systems.

5.7 If you detect any virus this must be reported immediately to the Head Teacher (this rule shall apply even where the anti-virus software automatically fixes the problem).

6.0 ACCESS SECURITY

6.1 All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

6.2 The School has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the School's network. The School also teach individuals about e-safety to ensure everyone is aware of how to protect the School's network and themselves.

6.3 All IT Systems (in particular mobile devices) shall be protected with a secure password or passcode, or such other form of secure log-in system as approved by the IT Department. Biometric log-in methods can only be used if approved by the IT Department.

6.4 All passwords must, where the software, computer, or device allows:

a) be at least 6 characters long including both numbers and letters;
b) be changed on a regular basis [and at least every 180 days];
c) cannot be the same as the previous 10 passwords you have used;
d) not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events, or places etc.)

6.4 Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the Head Teacher as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

6.5 If you forget your password you should notify the Head Teacher to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

6.6 You should not write down passwords if it is possible to remember them. If necessary, you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

6.7 Computers and other electronic devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this time period or disable the lock.

6.8 All mobile devices provided by the School, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

6.9 Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

6.0 DATA SECURITY

6.1 Personal data sent over the School network will be encrypted or otherwise secured.

6.2 All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Head Teacher who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given, all files and data should always be virus checked before they are downloaded onto the School's systems.

6.3 You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the School's Wi-Fi provided that you follow the school's requirements and instructions governing this use. All usage of your own device(s) whilst connected to the School's network or any other part of the IT Systems is subject to all relevant School Policies (including, but not limited to, this policy). The Head Teacher may at any time request the immediate disconnection of any such devices without notice.

7.0 ELECTRONIC STORAGE OF DATA

7.1 All portable data, and in particular personal data, should be stored on encrypted drives using methods recommended by the management team.

7.2 All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

7.3 You should not store any personal data on any mobile device, whether such device belongs to the School or otherwise without prior written approval of the Head Teacher. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the School's computer network in order for it to be backed up. This can be accessed by VPN when off site.

7.4 All electronic data must be securely backed up by the end of the each working day and is done by the IT Technician.

8.0 HOME WORKING

8.1 You should not take confidential or other information home without prior permission of the Head Teacher and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

8.2 When you have been given permission to take confidential or other information home, staff should adhere to the school's 'Working from Home Protocols' (Appendix 1).

8.3 You must ensure that:

a) the information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and

b) all confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

9.0 COMMUNICATIONS, TRANSFERS, INTERNET AND EMAIL USE

9.1 When using the School's IT Systems you are subject to and must comply with the School's Electronic Information and Communication Systems Policy.

9.2 The School work to ensure the systems do protect pupils and staff and are reviewed and improved regularly.

9.3 If staff or pupils discover unsuitable sites or any material which would be unsuitable, this should be reported to the Head Teacher.

9.4 Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the School cannot accept liability for the material accessed or its consequence.

9.5 All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by tracked DX (document exchange) or recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

9.6 Postal, DX, fax and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

9.7 You should be careful about maintaining confidentiality when speaking in public places.

9.8 You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the School.

9.9 Personal or confidential information should not be removed from the School without prior permission from Senior Management, except where the removal is temporary and necessary.

9.9.1 When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) not transported in see-through or other un-secured bags or cases;
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

10.0 REPORTING SECURITY BREACHES

10.1 All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Head Teacher. All members of staff have an obligation to report actual or potential data protection compliance failures.

10.2 When receiving a question or notification of a breach, the Head Teacher shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

10.3 Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Head Teacher. Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Head Teacher.

10.4 Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to Head Teacher.

10.5 All IT security breaches shall be fully documented.

10.6 Full details on how to notify of data breaches are set out in the Data Breach Policy.

ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

11.0 RELATED POLICIES

Staff should refer to the following policies that are related to this Information Security Policy:

- Electronic Information and Communication Systems Policy;
- Data Breach Policy;
- Data Protection Policy

Signed

Chair of the Governing Board

Date: **Review Date:**

ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

APPENDIX 1: WORKING FROM HOME PROTOCOLS

G.D.P.R: Working from home protocols

- **Be Vigilant – No one in your household should have access to or see the personal data you are using**

1. Be aware of your surroundings and who may be able to view your screen/work.
2. Do not write down your passwords on paper where they can be discovered.
3. Use strong passwords to protect your work devices and make sure you use a password that no-one else in the household knows or can guess.

- **Remember your data protection training to help you to ensure that everything is kept safe whilst at home**

Protecting student and staff data must remain the highest priority. Data breaches can cause real and significant harm to individuals and the risk of data breaches become much higher when data is accessed remotely or on a portable device.

- **Ensure that you use devices provided by the school rather than your own device to access the school's network**

Own devices should only be used with agreement from the IT team. This will help prevent unknown risks to the school's network (such as malware or security breaches). In addition to this: -

1. Check that your device is fully up to date with anti-virus, firewall, malware and security updates.
2. Ensure that work documents are saved on the school network securely rather than on the desktop or in "my documents."
3. Ensure your device has a password or (for tablets/phones) pin code. Passwords should be complex (a mixture of numbers, letters and capitals).

- **Two-factor authentication helps us ensure that access to school networks are done securely.**

By entering a passcode sent to an alternative device (such as a mobile phone) enables us to verify it is in fact you who is trying to log in. This is to ensure additional security.

- **Lock your screen while you are away/not using your device**

Please be vigilant to lock screens when not in use for long periods or where you are stepping away from your device. In addition, devices should be shut down at the end of the day.

- **Ensure that school IT equipment is kept in a secure place**

It is your responsibility to ensure that school equipment is kept secure (for example in a locked draw). If a device becomes lost or stolen, please report this to the school without delay and within 72 hours.

ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

- **Do not use your own USB memory sticks and plug them into school devices to take data from school systems or to upload data or documents to school systems**

This goes for memory sticks, pen drives, external hard drives. They should not be plugged into school devices unless they are issued/approved by the school IT team.

- **Do not install or download any software onto a work device without the approval of the school.**

Where approval is given, they should also be virus checked before they are downloaded onto the school's systems.

- **Ensure that if you are communicating remotely via video conferencing with your colleagues or students that:**

1. You use platforms which have been approved by the school.
2. Ensure that webcams are only activated when they need to be.
3. Do not record unless authorised to do so by the school (and the participants to the call also consent).

- **Always be careful which websites you visit and which emails attachments you open.**

1. Be careful when opening attachments to emails - even if the message appears to be from someone you know. Email attachments infected with viruses are one of the most widely used methods for infecting PCs.
2. Be vigilant against phishing attacks claiming financial rewards or encouraging charity donations. Phishing emails can look like they came from a real company or person you know and trust. The sole purpose of a phishing email scam is to trick you into going to a fake website that looks equally authentic and inputting personal information that would in turn provide the criminal with access to your accounts.
3. Remember that text, music and other content on the internet are copyright works. You should not download or email such content to others unless certain that the owner of such works allows this.

- **Ensure not to give out your personal details, such as a mobile phone number and personal email address to pupils.**

Do not use personal email accounts or numbers for school use.

- **Ensure you keep your own shared area and own email accounts organised.**

Do not keep emails or documents for longer than you need and it is each individual's responsibility to ensure their accounts are organised appropriately. If necessary, check the school's retention policy and schedule and ensure that you are complying with it and not storing personal data longer than you are allowed to.

ELMS FARM PRIMARY SCHOOL INFORMATION SECURITY POLICY

- **Paper records count too**

1. Paper documents taken from school or printed off at home must be kept secure at home just as they would be at school.
2. At the end of the working day, or when you leave your workstation unoccupied, all paper documents containing personal information need to be securely locked away to avoid unauthorised access.
3. You must ensure that documents are returned to secure storage at school as appropriate or they are destroyed securely at home. (see school's retention policy).
4. Do not put confidential waste into the ordinary waste. Ensure that it is shredded first.

Do report any breaches of the above to your line manager and refer to our acceptable use policies.

ELMS FARM PRIMARY SCHOOL DATA RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD
Employment Records	
Job applications and interview records of unsuccessful candidates	Six months after notifying unsuccessful candidates, unless the school has applicants' consent to keep their CVs for future reference. In this case, application forms will give applicants the opportunity to object to their details being retained
Job applications and interview records of successful candidates	6 years after employment ceases
Written particulars of employment, contracts of employment and changes to terms and conditions	6 years after employment ceases
Right to work documentation including identification documents	6 years after employment ceases
Immigration checks	Two years after the termination of employment
DBS checks and disclosures of criminal records forms	As soon as practicable after the check has been completed and the outcome recorded (i.e. whether it is satisfactory or not) unless in exceptional circumstances (for example to allow for consideration and resolution of any disputes or complaints) in which case, for no longer than 6 months.
Change of personal details notifications	No longer than 6 months after receiving this notification
Emergency contact details	Destroyed on termination
Personnel, disciplinary and training records	While employment continues and up to six years after employment ceases
Annual leave records	Six years after the end of tax year they relate to or possibly longer if leave can be carried over from year to year
Consents for the processing of personal and sensitive data	For as long as the data is being processed and up to 6 years afterwards
Working Time Regulations: • Opt out forms • Records of compliance with WTR	• Two years from the date on which they were entered into • Two years after the relevant period
Allegations of a child protection nature against a member of staff including where the allegation is founded	10 years from the date of the allegation or the person's normal retirement age (whichever is longer). This should be kept under review. Malicious allegations should be removed.

ELMS FARM PRIMARY SCHOOL DATA RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD
Financial and Payroll Records	
Pension records	12 years
Retirement benefits schemes – notifiable events (for example, relating to incapacity)	6 years from the end of the scheme year in which the event took place
Payroll and wage records	6 years after end of tax year they relate to
Maternity/Adoption/Paternity Leave records	3 years after end of tax year they relate to
Statutory Sick Pay	3 years after the end of the tax year they relate to
Current bank details	Until replaced/updated plus 3 years
Agreements and Administration Paperwork	
Collective workforce agreements and past agreements that could affect present employees	Permanently
Trade union agreements	10 years after ceasing to be effective
School Development Plans	3 years from the life of the plan
Visitors Book and Signing In Sheets	6 years
Newsletters and circulars to staff, parents and pupils	1 year (and the School may decide to archive one copy)
Health and Safety Records	
Health and Safety consultations	Permanently
Health and Safety Risk Assessments	Life of the risk assessment plus 3 years
Any records relating to any reportable death, injury, disease or dangerous occurrence	Date of incident plus 3 years provided that all records relating to the incident are held on personnel file
Fire precaution log books	6 years
Medical records and details of: - • control of lead at work • employees exposed to asbestos dust • records specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry made in the record
Records of tests and examinations of control systems and protection equipment under COSHH	5 years from the date on which the record was made

ELMS FARM PRIMARY SCHOOL DATA RETENTION SCHEDULE

FILE DESCRIPTION	RETENTION PERIOD
Temporary and Casual Workers	
Records relating to hours worked and payments made to workers	3 years
Pupil Records	
Details of whether admission is successful/unsuccessful	1 year from the date of admission/non-admission
Admissions register	Entries to be preserved for three years from date of entry
School Meals Registers	Current year plus 3 years
Free School Meals Registers	Current year plus 6 years
Pupil Record	Primary – Whilst the child attends the School
Attendance Registers	3 years from the date of entry
Special Educational Needs files, reviews and individual education plans (this includes any statement and all advice and information shared regarding educational needs)	Until the child turns 25.
Emails	2 years
Other Records	