Milverton Primary School

Security Policy, Arrangements & Procedures

Agreed by:	Premises Committee
Date Agreed:	June 2021
Date to be reviewed:	June 2024
Updated:	Issue #2 June 2021 (small alterations)

Table of Contents

Section 1:The Policy

1.1 Policy Statement

Milverton Primary School is committed to providing a safe and secure working, teaching and learning environment for all staff, pupils, governors, contractors and visitors whilst on site. Security of the school's resources, assets, information and systems is central to the sustained provision of quality educational services and their development.

Lack of security can affect health and accidents which compromise personal security. Security of and access to school information systems and files may affect not only the school but have potentially serious consequences to individuals and reputation. Prevention of accidents and health & safety are also important and dealt with by separate policies, risk assessment and procedures where appropriate. These documents are referred to as necessary for the role or task undertaken within school

Governors believe that consideration of security issues and management of risk is important. Together with forward planning to mitigate risks and anticipate response to the range of potential safeguarding and personal safety of persons using the premises as well as reducing loss to buildings and school resources will lead to a safe and more secure working environment. This will in turn allow available resources and time to be better utilised.

Personal safety, organisational security and ultimately safety of the school will only be attained where all parties join together in maintaining safe working conditions. The school understands that whilst there is a need to promote an open and welcoming environment, there is also a responsibility to address security and personal safety related issues. Attention to security will ensure protection of the school, staff, pupils, visitors and contractors, to provide a secure environment in which to work and study as well as protect physical assets and IT provision.

1.2 Core Elements

1. Organisational commitment to properly maintain staff and others safety and security
2.Procedures for use and activities to reduce risk and for staff at risk
3. Commitment to looking after other people, the working environment and resources by awareness of risks to the security and potential for loss and taking reasonable steps and precautions to minimise risk.

The aims this policy seeks to address are:

- to encourage and develop a positive and safe culture
- to ensure individuals feel safe
- to protect assets and property
- to mitigate and manage threats and reduce fear of these
- to communicate to staff, volunteers and governors the need to recognise the importance of sensible and proportionate actions and procedures to protect and safeguard
- to promote awareness and a common sense approach for individuals to protect themselves, colleagues and those for whom they have a duty of care
- to develop appropriate strategies, procedures and apportion relevant budget provision in accordance with risk and other relevant factors

All references in this policy to staff, parents, pupils, visitors or any persons involved with the school include people of any gender or collective responsibility. Therefore reference to parents also includes carers or adults with legal responsibility for pupils of this school.

<u>Section 2: Responsibilities and Obligations</u>

2.1 Introduction

Security within the school is the responsibility of everyone on site. Regular checks, self-assessments are carried out during the academic year with additional periodic inspection by external advisors from WES Safety & Premises. Results are reported to the governing body and used to assist with security planning and updating of the Security Policy, procedures and other relevant policies, such as Data Protection, Safeguarding and ICT Policies.

Security processes will also support the School's emergency and contingency planning together with useful documentation, such as inventory/asset registers required as part of the School's Business Continuity/Disaster Recovery Plan.

Staff will be informed of the school's security arrangements both formally and informally and updated with any security issues if or when they occur. This will be done through Staff briefings, team meetings, staff notice board/email and through the staff induction process for all new staff.

The Security Policy will be held on the school website.

2.2 Accountability and Responsibilities

- The Security Policy forms part of the schools Health and Safety Policy Arrangements and is supplemented and supported by other policies and procedures which are available to all staff. These include:
    - Visitor Health and Safety Information
    - Data Protection and Freedom of Information Policy
    - Safeguarding Policy
    - Staff Behaviour (Code of Conduct) and Whistle Blowing Policies
    - Pupil Behaviour Policy
    - Privacy Impact Assessment for Installation/Use of CCTV
    - E-Safety, Acceptable Use, Use of Mobile Devices, Internet and IT Policies
    - Recording and Use of Images/Photography Policy/Guidance

- The 'School Leadership Team', (SLT) as defined in the Health and Safety policy Management Structure will be responsible for implementing and reviewing the policy.

- The SLT are responsible for communicating policy, procedures and for monitoring security arrangements and procedures and for disseminating information or alerts that may increase the risk or vulnerability to people or the premises. Tasks to be delegated as appropriate.

- Governors are responsible for examining security risk, planning and reviewing financial expenditure to provide adequate resources for staff and assets to become safe and secure.

- The site manager is responsible for checking and maintaining the physical security of the premises which include but not limited to: the boundaries, gates, doors, locks and entry codes, alarm, sensors and bell boxes, external lighting and timed lights, security of waste and waste areas.

- The Headteacher is responsible for Data Protection and Freedom of Information where it may affect the protection of personal or sensitive data; see details in separate Data Protection Policy. Day to day management, maintaining accurate and adequate records processed fairly and lawfully including access requests is the responsibility of Matt Fisher, Headteacher

2.3 Review of Policy and Procedures

The Security Policy and any accompanying procedures will be reviewed on an annual basis, or sooner in the event of an incident or change that could affect security or safeguarding.

Policy Date ______________________________ Review Date ________________

Section3: Physical Security Arrangements

3.1 Access control

- See **Appendix A** for the site opening/closing details.
- During normal school hours access to the site and buildings will be restricted to the main reception entrance
- All gates and access routes will be secure or locked as specified:
  - Pedestrian gates are locked during the hours 9.00am -15.15pm
  - The gates opening the lane running through playground are locked between 8.00am and 17.00pm
- These times have been altered slightly to accommodate staggered pick up and drop off time times- restricting site access to families in the morning and using a one way drop off system during COVID19 restrictions

3.1.1 Entrances (site)

- The boundary is checked by site staff at least once per month
- During school hours pedestrian and vehicle gates to site will be opened and closed by site and office staff as specified below.
- No staff/visitor parking is allowed on site
- Access to play areas are controlled by securing access gates. See 3.1
- Site staff/administration staff are responsible for locking gates as 3.1.
- Arrangements for lettings or extended school activities are dealt with in Section 8.

3.1.2Entrances (Buildings)

- Signage will clearly display the main entrance from all access points.
- Additional signs are in place to direct to onsite Puddleducks nursery.
- Staff will use the main entrance at the start and end of the school day to sign in.
- Pupils will use designated entrances most appropriate to the classroom location.
- Pupils arriving after the start of school and registration will access their class via main reception and the school office to register arrival.
- External doors will be secure during the hours specified in section 3.1.

3.1.3Visitors (including school governors)

- Visitors are required to sign in with the school office before being given access to the school.
- Refuse collection workers have a key to Greartheed Road Gate, they alert the office for access through powered gate, workers come on site to collect bins, they do not sign in for this process, staff check to ensure workers have left site following collection and the gate has been secured after use.
- All visitors are given information relating to security requirements and their health and safety.
- Contractors will be given relevant information on the school's policy for "Contractors Working on Site"

- Staff will not afford access to any visitor that has not signed in at the Main Entrance.
- A Lanyard is issued to visitors that must be worn at all times. A red Lanyard is provided for visitros without suitable DBS check, a green lanyard for those who have provided this information.
- Visitors will be accompanied by a member of staff where practicable and reasonable.
- Contractors attending call outs and unplanned work will be escorted to the area of work. Staff in the vicinity of the work will be informed. Periodic checks will be made to see how work is progressing. See also Lone Working Policy and H & S Policy as applicable.

3.1.4 Staff

- Staff will sign in and out at the front office when arriving and leaving school premises. This procedure will apply also when the school is closed to pupils, including holidays and teacher training days.
- Staff will question any visitor, even if known, if a visitor Lanyard is not visible and/or not accompanied by another member of staff and ensure proper signing in systems have been followed.
- If a member of staff feels unsure about challenging any person on the premises they are to alert a member of the SLT immediately.

3.2 Keys and access authority

- Keys will be issued with the agreement of headteacher
- Master keys will be restricted to authorised site staff and SMT. Alarm codes are only shared with authorised staff responsible for keeping keys and alarm code secure.
- A key inventory will be maintained and reviewed annually, with a key audit undertaken every 3 years by the site manager.
- Keys not allocated to staff will be kept secure during the day and protected in an alarmed area over night, in the school office.
- All safe keys including exam store keys, will be locked away at night in the school office.

3.3 Access security

- Site/Facilities staff will check that external doors are secure at the end of the school day within 15 minutes of pupils vacating classrooms.
- Teaching staff will check at the start of the school day and after break times that the security measures on external doors are operational
- All staff will ensure that doors are secure at the end of the pupil day and that doors and windows to their areas are secured at the end of the working day.
- Site/Facilities staff are responsible for locking the building and activating the alarm when the building is unoccupied.
- Only authorised staff may activate and deactivate the intruder alarm.

- The management team, on at least an annual basis, will ensure the current measures are appropriate and adequate. This process will assess all access control measures to the site with the view to improvement where necessary.

Section 4: People and personal safety and security

The governors are committed to ensuring that staff, pupils and visitors may work and learn without fear or threat of verbal or physical abuse.

- WCC guidelines and School procedures are followed if an incident occurs and all incidents, including minor ones, are recorded and reported. HR and or disciplinary procedures will apply in staff conflict.
- The schools Building Emergency Evacuation Plan (BEEP) contains information on fire alarm system and evacuation procedures in the event of an emergency and can be found in the school office and staffroom notice board
- The school management team review access control measures regularly to include limited access out of school hours.
- Information and instruction will be given to both staff and pupils regarding the importance of personal and fire safety whilst on site. Regular evacuation practices and incident drills are undertaken.
- Parents/carers are required to sign an Acceptable Use Policy which outlines appropriate methods of communicating with the school and staff with a clear complaints procedure if required.
- Police are always involved in any incident that involves violence, a weapon or any other threat such as suspect packages.
- The schools "Emergency Advice and Support for Educational Establishments (E.A.S.E.E.) plan which contains school specific Emergency and Business Information can be found in the school office, orange file. Key members of school hold their own copy.

4.1 Pupil Safety & Security

- No pupil may leave the school premises during the school day unless personally collected by a parent/carer
- Children may walk home alone at the end of the school day in line with the schools set procedures and with signed agreement from parents
- School offsite procedures will apply for all school trips, educational visits and offsite activities. The schools "Educational Visits Coordinator" is Matt Fisher
- Any pupil leaving the school site during school hours must sign out at the front office before leaving and sign in again if they return before the end of the school day.
- Pupils are supervised during break and lunch-times. Playground procedures are in place and shared with staff.
- Pupils have designated internal and external social and activity spaces where break times are spent.
- Pupils are instructed on awareness of personal and internet safety as part of the PSHE, Computing curriculum and other study. See section on 7 on use of IT and Internet.
- Bullying and Cyberbullying is not acceptable behaviour and managed by e safety policy
- Pupils are required to sign up to the Acceptable Use Policy/e-safety policy
- Parents are invited to annual e-safety instruction sections provided free of charge.

- Pupils are updated and reminded about personal safety risks and stranger awareness principles as they are identified or alerts received.
- Parents are informed by email/newsletter/text of relevant security issues.
- Security of pupils with Special Educational Needs or a disability will have an individual risk assessment and appropriate strategies, such as learning or management plans in place.
- Other safeguarding issues are covered in Safeguarding , Staff Behaviour policies

4.2 Staff Safety & Security

Exterior lighting is installed by all access points.

- The school has adopted the WCC Personal Safety Policy.
- All staff should familiarise themselves with this policy.
- All staff considered at risk will have a risk assessment carried out prior to undertaking tasks.
- Any staff feeling at risk, fearing abuse or consider they have been a victim of abuse or the threat of abuse, should report any incidents and discuss role with headteacher
- There is an e-safety policy in place that includes procedures and sanctions for inappropriate use of internet communication.
- A Behaviour Policy is in place to support staff in managing behaviour.
- A “buddy” procedure has been adopted and will apply when staff work on their own, always on alarm response, or away from their normal place of work e.g. training/home visits.
- Instruction and training will be given to all Staff responsible for locking and unlocking school premises. Written procedures are provided and Staff must follow these when carrying out these duties. See the WCC Personal Safety Policy/ Schools Separate Lone Working Policy
- Alarm response is provided by Patrol Guard (08453705098), to avoid Lone Working risks to staff.
- Staff carrying out Alarm Response duties are provided with instruction and training, which must be followed on checking site and buildings when attending site on alarm activation. See Appendix C An example Alarm Call Out Procedures.

4.3 Lone Working

Lone working is minimised where possible and staff should always aim to be at work when others are present. The WCC Personal Safety Policy applies to all staff who may work in isolation or on their own and covers both term time, holiday working and home visits

- Personal Safety issues are included in the Lone Working Policy and individual/personalised risk assessments of which staff should be aware of and follow when working alone or in isolation.
- Additional procedures will apply for specific duties such as home visits and alarm response.
- Any lone working task not specifically included in job descriptions requires authority from headteacher prior to being undertaken.
- Staff undertaking lone working off site have additional training /procedures to follow.
- Staff undertaking tasks involving lone working have a personal risk assessment in place

- All lone working tasks are discussed/agreed with the management team.
- Requirements of our insurance provider will be followed in particular for all out of hours duties and “buddy” procedures.

4.4 Access to, Trespass and Barring on site

The school and grounds are private property and not for general public access during the stated times. The school is fairly unique in the lane running through the centre of the playground, requiring public access outside of the school day. Any person on site who has not signed in at Reception will be deemed a trespasser until identity verified.

- Staff should ask un-badged visitors to report to reception or leave the site.
- If a trespasser refuses to leave, causes a disturbance, or re-enters the site after leaving, the Headteacher should be notified, who will decide further action.
- Staff should avoid confrontation with trespassers and not approach them if they believe they may be at risk.
- Any person on site considered a danger to others or themselves will be immediately reported to the Police. The School’s EASEE plan will be implemented as required.
- Trespassers on site after school hours will usually be reported to the Police.
- The school follows Advice on school security: Access to, and barring of individuals from, school premises on barring individuals and will obtain legal advice as required to deal with nuisance or disturbance on school premises.

Section 5 : Security of Premises and Property

Governors ensure sufficient and relevant insurance cover is in place to cover both loss and damage to school property and contents. Asset Registers and inventories are in place and kept under review as part of the school's Business Continuity and EASEE plans. Personal property of staff and pupils is not insured and loss or damage is not the responsibility of the school.

A 24 hour monitored intruder alarm is installed with sensors covering all potential entry points into the buildings including doors, access to stairways, vulnerable areas such as stores where cash and ICT equipment is stored and potential points of entry from flat roofs.

5.1 Criminal damage including arson and break-in

If criminal damage occurs on site, personal safety and security for the site may have been breached.

- All damage to be reported to the Police, noting a crime number where required.
- WES Safety and Premises will be notified via the WES Security Incident Report form.
- Damage must be assessed to ensure that access control measures are still in place and that the damage will be attended to by Property/Maintenance contractors as quickly as possible.
- Temporary arrangements will be arranged to secure the building and site if damage cannot be fully repaired straight away.
- Insurance Company will be notified in accordance with policy requirements. If excessive damage done claim requirements must be checked before clear-up or reinstatement as evidence of extent may be required.
- A review of security measures will be carried out.

5.2 Safety of property

- All property and equipment exceeding an individual value of £1000 will be included on the School's Asset Register.
- All property and equipment will be visibly marked to identify the item as belonging to the school and as a deterrent to theft. See procedures Appendix B
- All ICT equipment will be recorded on the ICT inventory including unique serial numbers for identification and location of Smartwater.
- All laptops are encrypted using "Bitlocker" / specific Apple software
- All ground floor rooms, entrance lobbies or corridors leading to external doors will be protected by sensors connected to the intruder alarm system.
- The intruder alarm will be connected to a monitoring station at all times out of school hours.
- The alarm will be activated at all times outside of the school day. Where possible the alarm zoning facility will be used during lettings/lone working and/or out of hours activities, increasing security to unused buildings/rooms, also adding to the personal safety of staff at such times.
- Site staff will ensure that the alarm is in full working order by carrying out monthly visual checks of the system and sensors.

5.3 Personal Property

- Pupils should not bring personal property of value to school unless required for lessons e.g. music.
- Pupils leave items of value, including mobile phones, with the school office during school hours. Pupils are discouraged from bringing cash unless for a specified purpose.
- Staff are responsible for their own personal property whether in school or vehicles left on the school site, including items used in lessons, unless the school has agreed to cover these.
- Some secure lockers are provided in which staff may leave personal items.
- The school is not responsible for any personal items brought on site that are lost, stolen or destroyed by any means, including visitors/parent property. It is recommended household insurance cover is checked before personal items are brought to school if insurance is required.

5.4 Cash Handling and Management

- All cash on site is kept to a minimum and within insurance limits with regular banking of large amounts.
- Cash payments on site are limited to a maximum of £50 in any one transaction.
- All salary, expenses and invoices are paid directly into bank accounts only.
- The school subscribe to Parent Pay which reduces the requirement for handling, banking and securing cash.
- Cash must always be counted in a secure area. Staff are aware that cash is kept out of sight when visitors can view or are in the area where cash is dealt with.
- Only authorised staff are permitted to access keys to safes/petty cash and count, record and bank cash/cheques. Training and instruction is provided as appropriate.

5.5 Keys Security and Management

- At night safe keys are kept in a locked area separate from other keys.
- All site keys are stored in a locked key safe accessible to authorised staff only. Keys to external doors are stored in the key box.
- Keys to external doors are unidentifiable.
- A key inventory is maintained and updated annually by Site Manager.
- All keys issued to staff are recorded on an inventory and the responsibility of staff to keep safe and secure.
- Staff will notify the responsible person if keys are lost/stolen immediately and return keys when they are no longer required, on leaving the school and if requested to do so.

Section 6: Security of Data and Information

6.1 Use and Safe Storage of Personal, Sensitive Data

This policy is in reference to the schools data protection policy that meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

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

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

The school have specific obligations and it is important to keep personal details of staff, pupils and others secure.

All staff must be aware of the School's Data Protection policy and apply it to all personal information and images stored in paper files or electronically, in particular where there is responsibility for recording, managing and accessing personal information and data.

- The member of staff responsible for Data Protection is Matt Fisher. Responsibility includes raising general data protection awareness, staff training, writing, reviewing, monitoring and adherence to policy and procedures.
- The School's Data Protection Policy is regularly reviewed and monitored.
- The Register of Data Controllers Entry register is updated if personal information is processed differently or used for a new or different purpose, e.g. CCTV.
- The purpose(s) for holding data and retention periods will be reviewed with the DP Policy.
- Staff responsible for managing and keeping information up to date will receive training as appropriate. (See Data Protection Act Appendix D Glossary)
- All Personal data recorded will be stored, processed, transferred, deleted or destroyed and made available according to the DPA and school/employer policy. If staff forward personal information via email or fax secure procedures outlined in ICT policy will be followed.
- All personal and sensitive information stored electronically will be held in secure files which will be encrypted and/or password protected as appropriate, including archived records.
- Information stored in all other forms other than electronically including archived records, will be kept secure.
- Only authorised persons may access or process secure files. All authorised staff must keep passwords secure and not share these with any other person.
- Access to any personal/sensitive information is not permitted in a public place.
- All archiving, deletion or destruction of information will be in accordance with school procedures.
- No personal/sensitive information may be downloaded to any personal device
- Information downloaded will be protected. Only encrypted memory sticks provided by the school may be used

- Downloads onto mobile devices other than school equipment, which is password protected is not permitted.
- When using information staff must work in a secure environment and not a public place.
- The School backs up information systems on a daily basis using WES ICT Services
- In order to assist in managing the responsibility for all areas of data protection compliance for personal information stored off the school site the school follows DfE advice on the use of Cloud software.
- The school remains the data controller for all information stored by the CSP and has verified that the processing carried out by the CSP complies with the DPA and they may only act on the instruction of a duly authorised member of the school staff.
- There is a Data Processing Agreement with the Cloud services provider. The school's data handling requirements are confirmed by contract.
- A Privacy Impact Assessment is carried out when selecting services, processes, recording or monitoring systems that require DPA compliance
- A Fair Processing Statement or Privacy Notice to let people know how personal information is used or processed is maintained and kept reviewed. This is issued annually to staff/ parents/pupils and available on the school's website.

6.2 Freedom of Information Act Requirements and Publishing Information (FOIA) 2000

As required by the FOIA 2000 the school have adopted the ICO's Model Publication Scheme and this is published on the schools website.

- The member of staff responsible for Information Rights, including FOI requests is headteacher
- The School's Guide to Information is published alongside the Model Publication Scheme Available on request from the School Office
- Staff are informed what personal information may be supplied when dealing with a FOI request.
- The school will inform parents and pupils when publishing examination results including how and when this will be done, taking into account any objections prior to publication. Guidance provided by the ICO may be referred to as required.

6.3 Use of Biometric Information

The school does not collect or use Biometric information but will have due regard to the requirements of the Protection of Freedoms Act 2012 if used in the future.

6.4 Taking, use and storage of images

The school follows WSCB and WCC guidance concerning all aspects of Safeguarding including the use of all photographic and image capturing equipment. The school follows the Use of Images Guidance for Children and Young People in Warwickshire, available on the WSCB website resources page

- Equipment includes all mobile devices such as cameras, phones, wristbands, webcams, bodycams and unmanned aerial vehicles/drones.

- All staff should familiarise themselves with guidance before switching on a mobile device on school premises and always before taking photographs which include people.
- Visitors/contractors are not permitted to use mobile devices, including aerial device with image capturing capabilities while on school site. These should be switched off unless permission to use or take calls has been obtained from headteacher
- Contractors may only use mobile devices with cameras inside their work area or compound where the contract work area is separated from school work areas.
- Maintenance contractors are required to inform the school office when they sign in if they require a mobile device with a camera to remain switched on or intend to operate any UAV.
- Images are securely stored and used in accordance with school policy and the DPA.

6.5 Closed Circuit TV and Unmanned Aerial Vehicles (UAV)

CCTV is installed to monitor external areas of the school premises for the purposes of collecting visual images for the prevention and detection of crime and the apprehension or prosecution of offenders.

- The Site manager is responsible for the operation of CCTV, including training of staff authorised to view/access images and secure storage of images.
- A Privacy Impact Analysis (DPIA) has been carried out and will be reviewed annually or if changes or extension of the system are to be made.
- CCTV is operated in accordance with the 12 guiding principles of the ICO's "In the picture: A data protection code of practice for surveillance cameras and personal information". See Appendix 3 of code.
- CCTV may also be used for other purposes as deemed reasonable and appropriate, subject to a DPIA or other justification.
- Suitable and sufficient signage is placed around the site and buildings.
- Covert surveillance is undertaken in rare circumstances and only if authorised by the Headteacher and Chair of Governors. Guidance in the ICO's Employment Practices Code and other good practice will be followed.
- Anyone wishing to operate UAV on the school site for any reason including school use for curriculum, survey, or social reasons (hirers) will require express permission from headteacher
- A DPIA will need to be carried out prior to use of any UAV with due regard to the ICO code of practice on the use of surveillance cameras
- Images from UAV used on the school site are not permitted to be recorded. Without a justifiable reason and authorised by the Headteacher / Governing body
- Any images from UAV that include people will be kept secure as per Section 6 of this Policy.

6.6 Disposal/Destruction of Personal/Sensitive information and Data

Data is destroyed using safe and recommended systems relevant to the storage method and nature of the information.

- There will be an annual review of all documents/data and the retention period.

- Documents with personal or sensitive information will be disposed of in a timely manner to comply with GDPR Guidance
- Detailed procedures are included in the Data Protection Policy.
- All data whether stored electronically or on paper remains secure until destroyed.
- When using a specialist service provider to dispose of information a detailed written specification and order will be issued.
- All paper documents are shredded. Staff or a contractor are authorised by headteacher. All electronic data will be removed by certified providers / appropriately trained staff using approved method in Data Protection Policy

6.7 Disposal/Destruction of Assets

- Items that are either surplus to requirements, no longer required or used will be disposed of in accordance with school procedures. Items with a residual value will be sold or either offered for sale or collection in order to obtain best value.
- Items to be sold will be kept secure until collected. Sales, disposal and proceeds will be dealt with in accordance with financial standing orders or other relevant procedures.
- All disposals will record: method of disposal (sold/recycled/destroyed); new owner; specific actions such as removal of school identification and entered onto the school's inventory/asset register.
- All disposals with a residual value over £1000 require the authorisation of two members of staff, one of whom will be on the Senior Management Team and School Bursar.

6.7.1 IT Asset Disposal and Personal Data Deletion Strategy

The school recognises the obligation under principle 7 of the DPA and adopt appropriate measures to protect against accidental loss, destruction or damage to personal data. This is especially relevant when disposing of IT equipment.

- All information on computer hard drives is to be will be deleted on behalf of the school via a specialist asset disposal service provider.
- An arrangement for appropriate disposal/recycling is the responsibility of headteacher
- Cleaning/disposal carried out by a specialist service provider of school equipment or school information will be subject to a clear specification establishing who is responsible for deletion of data, if not the school, and a clear security protocol while cleaning is undertaken.
- All devices are to remain in a secure area while awaiting disposal or collection.
- A risk assessment has been carried out for disposal of personal/sensitive information.
- See School IT policy for detailed disposal requirements

Section 7: Use of IT, the Internet and Mobile Devices

The use of IT and the internet is a valuable tool both in terms of enhancing education and improving efficiency of administration tasks and access to information. However inappropriate use of this facility can put the school and/or individual at risk of loss of assets and reputation.

7.1 Use of IT and access to the internet

- All staff that manage or process personal information must refer to section 6 of this policy and the Data Protection Policy.
- There are acceptable use and e-safety policies for the internet that use that pupils/staff/and parents are required to read, sign and follow as appropriate to the media in use.
- Staff and governors are also made aware of the code of conduct in relation to use of IT.
- Information and guidance is provided to parents who are encouraged to monitor use of the internet at home.
- The IT policy/policies is the responsibility of the IT co-ordinator or headteacher to implement, monitor and review. Review is carried out annually or sooner if a serious breach of IT use or incident, such as a scam attack, occurs.
- To develop and maintain good practice in e-safety, the school has acquired the 360 degree Safer Online accreditation and is currently applying for renewal 2018.
- Staff and pupils are made aware that use of the internet is monitored and filters are in place to block the use of social media and other inappropriate websites.
- Breaches of the IT usage policy could result in disciplinary action and/or sanctions.

7.2 Use of mobile Devices

Mobile devices such as ipads are owned by the school and used by staff and pupils. Specific security procedures apply to the issue and return of devices to reduce the risk of theft or loss. See the school IT Policy

- All school devices have security software to track the location if stolen/lost and/or to wipe data in the event of theft or loss of the device.
- School business may not be conducted on a mobile device when connected to a public wifi.
- Use of school mobile devices is restricted to staff members only. Staff must keep all mobile devices safe and secure while off site and not leave them unattended under any circumstances, especially in cars and public places.
- Staff will consider whether email is secure when sending from a mobile device. No personal information will be sent from a mobile device unless encrypted.
- Staff may not connect personal devices to school equipment.
- Staff may not download school information to personal devices.
- Staff may not download school personal/sensitive information to personal devices.
- If personal devices are used for school work staff must follow guidelines and procedures in the school IT policy, with permission from the headteacher or in an emergency situation.

- No personal mobile may be used for school information.
- All mobile devices will be cleared and cleaned of school information prior to disposal, replacement and when staff leaves the school.
- For use of image capturing function of any mobile device refer to Section 6 of this Policy.

Section 8 Extended school Hours and Out of Hours Use by Hirers

The School governors encourage use of school facilities by the community and have taken the increased risks into account when agreeing the school's Hiring Policy and the Security Policy.

- All hirers must complete a hiring application form and the dates and purpose of hire agreed prior to use.
- Hirers will be informed of any areas which are not to be used or accessed during hirings
- Areas of the school not in use out of hours will remain alarm protected by use of the zoning facility of the alarm (main building, west hall, east hall).
- The Headteacher / Site Manager will be responsible for all hirings. All staff dealing with hirers should report any incidents involving hirers or occurring during out of hours use.
- Site staff will be made aware of all hirings and extended school use that occur outside normal opening hours.
- School staff and agreed contractors only remain responsible for alarm setting and locking and unlocking for use outside the hours specified in Appendix A.
- Staff carrying out locking/unlocking duties check hired areas are cleared, all internal doors are closed, all combustibles are removed or stored safely and that alarm sensors are working before activating the alarm and securing the buildings and site.
- Hirers are not issued with any keys or access codes to any part of the site or buildings without express permission of the governing body.

Appendix A Emergency contacts& School Opening Hours

Emergency Contacts

The schools EASEE Plan can be found in the Purple Folder in School Office for full emergency procedures and contacts.

Police	In an emergency – 999 Non-emergency 101 Dial 9 for outside line
Police Community Support Officer	PC Sam Stamford PC980 PC Andy Whiton PC1525 01926 684263 lsn.snt@warwickshire.pnn.police.uk
WES Safety and Premises	01926 412440wespremises@warwickshire.gov.uk Property Risk Manager 01926 476850 propertyrisk@warwickshire.gov.uk
Intruder alarm company details	Patrol Guard (08453705098), www.patrolguard.co.uk
Alarm Monitoring Company details@	Patrol Guard (08453705098), www.patrolguard.co.uk
CCTV company	SeeCam 07917508961
Resources – Property Hotline	01926 414123
Insurance Details	(WCC only) Insurance Officer – 01926 418160

School Opening Hours

	Time	Time
Gates	School Gates 8.50 Open Lane Gates 6.00pm Open	School Gates 4.30 Close Lane Gates 8.00am Close
Staff on site	6.30am In	6.30pm Out
Pupils on site	8.00 In	6.00pm Out
Hirings	Independent agreement	Independent agreement
Extended Services	School Gates 8.50 Open Lane Gates 5.00pm Open	School Gates 4.30 Close Lane Gates 8.00am Close

Appendix B School Property Marking Procedures

The school has chosen chemical forensic marking (Smart Water) to protect equipment and property

1	Staff responsible for security marking T Heard - Site Manager Staff responsible for asset register/inventories M Fisher - Headteacher
2	No equipment is to be distributed or be put into use prior to being marked with the school name/ post code / asset registration
3	Staff should check all new equipment for visible sign of security mark when first in use and periodically check it remains visible and not tampered with.
4	Equipment over the value of £1000 will be included in the asset register prior to distribution to teaching or administrative areas
5	All equipment will be marked on the front or a visible face of the equipment. If the equipment is to be placed in a jacket or protective sleeve e.g. notepad, the marking should be placed in the most visible location available or an additional notice/sticker placed on the cover to remind users the equipment is security marked
6	Responsible person will check the marking annually/bi –annually to ensure it remains in good condition and visible. (Note UV Pen and Smartwater on a flat or handled surface should be checked for wear annually)

Appendix C An example alarm call-out procedure

First contact is with alarm monitoring company who send out security officer.

If school staff contacted following procedure applies.
Assume the alarm activation is genuine.
Make immediate contact with the "Buddy" as per Lone Working Procedure.

1	Collect a mobile phone, powerful torch, checking batteries before leaving and high-viz tabard/jacket.
2	On arrival at site, if buddy not present confirm arrival. Using the torch, walk round the entire outside of the school. Check windows and doors, especially behind shrubs for signs of entry or disturbance.
3	If no signs of entry unlock building to check alarm panel. If any signs of entry to the building or suspicious of entry contact Police and do not enter building.
4	If buddy not present, make direct contact to confirm whether entering the building or contact made with Police.
5	If Police called wait for arrival in an open, well-lit place or follow police instruction or investigate source and or cause of activation after silencing alarm and checking panel.
6	Reset alarm following any action to rectify cause of activation. If alarm has fault or unable to reset call alarm company using emergency contact list.

Note: details from the insurance provider should be followed for the inclusion of "buddy's" in the schools public liability cover.

Appendix DGlossary

Abbreviation	Title or Description	Contact or other Information
BYOD	Bring Your Own Device	https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf
CCTV	Closed Circuit Television	https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
CSP	Cloud Service Provider	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447911/Cloud_services_software_dept_advice_July_23_2015.pdf
DfE	Department for Education	https://www.gov.uk/government/collections/departmental-advice-schools
DPA	Data Protection Act 1998	1. https://ico.org.uk//for-organisations/guide-to-data-protection/ 2 https://ico.org.uk/media/for-organisations/documents/1130/summary_report_dp_guidance_for_schools.pdf
FOIA	Freedom of Information Act	https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/ https://www.gov.uk/make-a-freedom-of-information-request/the-freedom-of-information-act
ICO	Information Commissioner's Office	www.ico.org.uk
PIA	Privacy Impact Analysis	https://ico.org.uk/media/1595/pia-code-of-practice.pdf
UAV	Unmanned aerial vehicles aka drones	https://ico.org.uk/media/1542/cctv-code-of-practice.pdf
WCC	Warwickshire County Council	http://www.warwickshire.gov.uk
WES	Warwickshire Education Services	https://apps.warwickshire.gov.uk/Wes/
WSCB	Warwickshire Safeguarding Children Board	http://www.warwickshire.gov.uk/aboutwscb

Appendix ESources of guidance

	Title	Link to Document
ICO	Publication of Exam Results	https://ico.org.uk/media/for-organisations/documents/1135/publication-of-exam-results-by-schools-dpa-guidance.pdf
ICO	Model Publication Scheme to adopt	https://ico.org.uk/media/for-organisations/documents/1153/model-publication-scheme.pdf
ICO	Definition document for the governing bodies of maintained and other state-funded schools	https://ico.org.uk/media/for-organisations/documents/1235/definition-document-schools-in-england.pdf
ICO	Guide to Information – Template for small schools How to complete the Guide to Information	https://ico.org.uk/media/for-organisations/documents/1278/schools_england_mps_final.doc https://ico.org.uk/media/for-organisations/documents/1242/how-to-complete-template-guide-to-info-for-schools.pdf
ICO	Guidance on disclosing information safely by removing personal data – applies to both access requests (DPA) and Freedom of Information requests	https://ico.org.uk/media/for-organisations/documents/how-to-disclose-information-safely-removing-personal-data-from-information-requests-and-datasets/1432979/how-to-disclose-information-safely.pdf
DfE	DfE Advice on the use of Cloud software and a cloud service provider	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/447911/Cloud_services_software_dept_advice_July_23_2015.pdf
DfE	Protection of Biometric Information of Children in Schools	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268649/biometrics_advice_revised_12_12_2012.pdf
DfE	Advice on school security: Access to, and barring of individuals from, school premises	https://www.gov.uk/government/publications/school-security
DfE	Behaviour and Discipline in Schools	https://www.gov.uk/government/publications/behaviour-and-discipline-in-schools
DfE & WCC	Fair Processing or Privacy Notices	http://www.warwickshire.gov.uk/schoolprivacynotices https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices
ICO	Asset Disposal for Organisations	https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf
ICO	Employment Practices Code (refer to for use of covert CCTV)	https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf