Stockingford Nursery School

School and the Building Security Policy, Procedures & Arrangements

Headteacher: R. C. Ellis **Date:** 26.11.24

Chair of Governors: C S Phillips **Date:** 26-11-24

Version: 3
Date Issue: July 2024
Review: July 2025

Table of Contents

Section 1: The Policy 4
1.1 Policy Statement 4
1.2 Core Elements 4
Section 2: Responsibilities and Obligations 5
2.1 Introduction 5
2.2 Accountability and Responsibilities 5
2.3 Review of Policy and Procedures 6
Section 3: Physical Security Arrangements 7
3.1 Access control 7
3.1.1 Entrances (site) 7
3.1.2 Entrances (Buildings) 7
3.1.3 Visitors (including shool governors/trustees) 7
3.1.4 Staff 8
3.2 Keys and access authority 8
3.3 Access security 8
Section 4: People and personal safety and security 9
4.1 Pupil Safety & Security 9
4.2 Staff Safety & Security 10
4.3 Lone Working 10
4.4 Access to, Trespass and Barring on site 11
Section 5 : Security of Premises and Property 12
5.1 Criminal damage including arson and break-in 12
5.2 Safety of property 12
5.3 Personal Property 13
5.4 Cash Handling and Management 13
5.5 Keys Security and Management 13
Section 6: Security of Data and Information 14
6.1 Use and Safe Storage of Personal, Sensitive and *Biometric Information and/or Data 14
6.2 Freedom of Information Act Requirements and Publishing Information (FOIA) 2000 14
6.3 Use of Biometric Information 15
6.4 Taking, use and storage of images 15
6.5 Closed Circuit TV and Unmanned Aerial Vehicles (UAV) 15
6.6 Disposal/Destruction of Personal/Sensitive information and Data 16
6.7 Disposal/Destruction of Assets 16

6.7.1 IT Asset Disposal and Personal Data Deletion Strategy 17
Section 7: Use of IT, the Internet and Mobile Devices 17
7.1 Use of IT and access to the internet 17
7.2 Use of mobile Devices 18
Section 8 Extended School Hours and Out of Hours Use by Hirers 18
Appendix A Emergency contacts & School Opening Hours 20
Appendix B School Property Marking Procedures 21

Section 1: The Policy

1.1 Policy Statement

Stockingford Nursery 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 Schools 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 and the building 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 and the building 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.

Section 2: Responsibilities and Obligations

2.1 Introduction

Security within the School and the building 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 such as 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 emergency planning, 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 and the building'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 email and through the staff induction process for all new staff.

The Security and Building Policy will be held in the School office.

2.2 Accountability and Responsibilities

- The Security and Building Policy forms part of the School's Health and Safety Policy Arrangements and is supplemented and supported by other policies and procedures which are available to all staff.

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

- The SLT will be 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 Caretaker 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 Data Protection Officer (WCC) is responsible for providing guidance on data protection standards. The School's information and data protection policies can be found in the School office. Day to day management is the responsibility of Katherine King.

- The School Business Manager is responsible for electronic entry/security devices including issuing, deleting lost or returned devices and maintaining a record of entry fobs. They can also produce reports of fob usage/ doors left open, issue temporary entry fob/card for contractors/visitors as directed, manage and record normal servicing of the system and malfunction, issuing orders for repairs in accordance with procedures.

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.

Section 3: 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 the building will be restricted to the main reception entrance via one pedestrian gate and the main vehicle entrance and car park.
- All gates and access routes will be secure or locked as specified:
  - Pedestrian and vehicle gates are locked during the hours 7pm – 6am.
  - Gates to play areas are locked.

3.1.1 Entrances (site)

- The School and building sign is clearly visible from the main access route and signage directs visitors to the main entrance to use for access to the School and building.
- The boundary is checked by site staff at least once per day.
- Staff and Integrated partners frequently delivering services from the building are allowed to park in the staff and visitors car park.
- Site staff/Nursery Staff are responsible for locking gates as 3.1.
- Arrangements for lettings or extended School activities are dealt with in Section 8.

3.1.2 Entrances (Buildings)

- Signage is clearly displayed indicating the main entrance from all access points.
- Staff will use the main entrance to sign in on arrival.
- Pupils arriving after the start of School and registration will access their classrooms via main reception to register arrival.
- External gates/doors will be secure during the hours specified in section 3.1.

3.1.3 Visitors (including School Governors)

- Visitors are required to sign in with Reception before being given access to the School / building.
- All visitors are given information relating to security requirements and their health and safety. Contractors will also be given relevant information on the Building's policy for Contractors Working on Site.
- Staff will not afford access to any visitor that has not signed in at Reception.
- A badge is issued to visitors that do not have a photo ID badge and must be worn at all times.
- 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 Reception when arriving and leaving the building. This procedure will apply also when the building is closed to pupils or the public, including holidays and teacher training days.
- Staff identity badges must be worn at all times whilst in the building.
- Staff will question any visitor, even if known, if a visitor badge 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 senior leadership team immediately.

3.2 Keys and access authority

- Staff are required to wear their photo identity badge, and also have access to a fob key. These must be kept safe and not loaned to any other person, including other members of staff.
- If any badge, key or fob is lost this should be reported immediately to the Headteacher or the School Business Manager.
- Keys will be issued with the agreement of the Headteacher.
- Master keys will be restricted to authorised site staff. 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 three years.
- Keys not allocated to staff will be kept secure during the day and protected in an alarmed area over night.
- The School safe is secured with a code. The library safe is opened with a key which Library staff are responsible for.

3.3 Access security

- All exit doors are fitted with automatic security locks that allow free egress in an emergency
- Site/Facilities staff will check that external doors are secure at the end of the day.
- All staff will ensure 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 senior leadership 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, children, families and visitors may work and learn without fear or threat of verbal or physical abuse.

- WCC guidelines and building 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 Buildings Emergency Evacuation Plan contains information on fire alarm system and evacuation procedures in the event of an emergency and can be found in the School office and in emergency grab bags.
- The senior leadership team review, in discussion with the building user group, access control measures regularly.
- Information and instruction will be given to both staff, visitors, children and families 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 a consent form 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 "Emergency Advice and Support for Educational Establishments" (E.A.S.E.E.) plan which contains building specific Emergency and Business Information can be found in the School office.

4.1 Pupil Safety & Security

- No pupil may leave the building unless personally collected by a parent / carer, or authorised named person given by the parent / carer.
- Once children are in the building at the start of their session they are not permitted to leave the premises until the end of the session unless prior arrangements have been made by parents/carers.
- School offsite procedures will apply for all School trips, educational visits and offsite activities. The Schools "Educational Visits Coordinator" is the Headteacher - Katherine King and Nursery Teacher Sally Phillips.
- Any pupil leaving the School site during School hours must be signed out on the classroom registers before leaving and sign in again if they return before the end of the School day.

- Pupils are instructed on awareness of personal and internet safety as part of the PSHE, computing curriculum and other study as developmentally appropriate. See section on 7 on use of IT and Internet.
- Bullying and Cyberbullying is not acceptable behaviour and managed by the Behaviour Policy and the Online Safety Policy.
- Parents /carers are made aware of online safety procedures and good practice through Facebook, newsletters and displays/posters in the building.
- Pupils are updated and reminded about personal safety risks and stranger awareness principles as developmentally appropriate, as they are identified or alerts received.
- Parents are informed by letter/newsletter/MySchoolApp 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 and Staff Behaviour policies and are located in the office.

4.2 Staff Safety & Security

Exterior lighting is installed by all access and egress areas including the car park and other vulnerable areas.

- The School and Library have adopted the employer 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 or discuss role with a member of the Senior Leadership Team.
- There is a School Online Safety Policy in place that includes procedures and sanctions for inappropriate use of internet communication.
- A School pupil 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, 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. Procedures are in place and staff must follow these when carrying out these duties. See the WCC Personal Safety Policy / Lone Working Policy.
- Alarm response is provided by Coventry City Council to avoid Lone Working risks to staff.

4.3 Lone Working

Lone working is minimised where possible and staff should always aim to be at work when others are present. The Employer Personal Safety Policy applies to all WCC 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 for the School 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 the Headteacher prior to being undertaken.
- Should Staff undertake lone working off site they would have additional training / procedures to follow.
- Should Staff undertake tasks involving lone working there should be a risk assessment in place.
- All lone working tasks are discussed/agreed with the Senior Leadership Team.
- Requirements of our insurance provider will be followed in particular for all out of hour's duties and "buddy" procedures.

4.4 Access to, Trespass and Barring on site

The building and grounds are private property and not for general public access. Any person on site who has not signed in at reception will be deemed a trespasser until identity is verified.

- Parents are permitted a right of entry to designated areas, to collect and drop off pupils at the start and end of session. Other times should be made by prior arrangement.
- The building car park may only be used by staff/visitors/contractors and deliveries.
- Parents must not bring cars on the School site.
- Staff should ask un-badged visitors to report to reception.
- If a trespasser refuses to leave, causes a disturbance, or re-enters the site after leaving, the Senior Leadership Team 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 buildings EASEE plan will be implemented as required.
- Trespassers on site after opening hours will be reported to the Police.

The building follows Advice on School security: Access to, and barring of individuals from, building premises on barring individuals and will obtain legal advice as required to deal with nuisance or disturbance on building 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.
- Where appropriate 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 reinstated straight away.
- Insurance Company will be notified in accordance with policy requirements. If excessive damage is 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 fixed assets will be included on the School's Asset Register as per DfE Good Estates Management Guidance (https://www.gov.uk/guidance/good-estate-management-for-schools).
- All valuable/portable property and equipment will be visibly marked to identify the item as belonging to the School and as a deterrent to theft. There is a written procedure – please see Appendix B
- All ICT equipment will be recorded on the ICT inventory including unique serial numbers for identification and location of Smartwater and/or chemical etching.
- 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 hour's activities, increasing security to unused buildings/rooms, also adding to the personal safety of staff at such times.
- Site/caretaking staff will ensure that the alarm is in full working order by carrying out daily/weekly/monthly visual checks of the system and sensors.

5.3 Personal Property

- Pupils should not bring personal property of value to School.
- 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 £250 in any one transaction.
- All salary, expenses and invoices are paid directly into bank accounts only.
- All cash/cheques are collected and banked in line with the cash handling risk assessment
- 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.
- A cash handling activities risk assessment has been carried out is included in the Office Activities Risk Assessment.

5.5 Keys Security and Management

- All site keys are stored in a key safe accessible to authorised staff only. Keys to external doors are stored in the secure room overnight.
- The keys are coded using alphabetical order with a corresponding list.
- A key inventory is maintained and updated bi-annually by the administration assistant, but updated as and when required.
- All keys issued to staff are recorded on an inventory and the responsibility of staff to keep safe and secure, and not labelled with School details.
- Staff will notify the Headteacher 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.

- Staff keys remain the responsibility of the individual and must not be lent to anyone else.
- Staff may not copy the keys under any circumstances, without prior permission from the Headteacher.
- Where keys are issued to external persons/groups the Site Responsible Person should ensure reasonable control measures are put in place including a key holder agreement

Section 6: Security of Data and Information

6.1 Use and Safe Storage of Personal, Sensitive and Biometric Information and/or Data

The School aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). See the Schools Data Protection Policy in the office.

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 point(s) of contact for queries is the Headteacher.
- Information downloaded will be protected. See DP/Online Safety Policy. Only encrypted memory sticks provided by the School may be used if required. 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 etc.
- Staff are permitted to use personal devices for work, e.g. accessing email. See Online Safety Policy and guidance on ICO Website.
- 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.

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 School's website.

- The member of staff responsible for Information Rights, including FOI requests is the 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 the DPO, Warwickshire Safeguarding Children Board (www.safeguardingwarwickshire.co.uk) and employer guidance concerning all aspects of Safeguarding including the use of all photographic and image capturing equipment. Equipment includes all mobile devices such as cameras, phones, wristbands, webcams, bodycams and unmanned aerial vehicles/drones.

- All staff should familiarise themselves with guidance / the policy before switching on a mobile device on School premises and always before taking photographs which include people.
- Visitors are permitted to use mobile devices whilst in the building in designated areas. Visitors may not take photographs of any children in the Nursery School or the Children and Family Centre on their mobile phone.
- 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 unmanned aerial vehicle (UAV).
- Images are securely stored and used in accordance with School Data Protection policy and the Data Protection Act

6.5 Closed Circuit TV and Unmanned Aerial Vehicles (UAV)

CCTV is presently installed on School premises but is not operational. If this is considered necessary advice will be sourced from the DPO, a Privacy Impact Assessment (PIA) will be carried out and current Information Commission's Office / DfE guidance will be used in the planning stages.

Where CCTV is installed it is recommended the arrangements are recorded detailing how the School is complying with the current Information Commissioner's Office (ICO) Code of Practice (see the ICO website - https://ico.org.uk/ and search CCTV).

- Covert surveillance is undertaken in rare circumstances and only if authorised by the Headteacher. 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 the Headteacher.
- A PIA 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.
- 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

See School Data Protection and Information Security Policy, seek further guidance from the Schools DPO if required.

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

- There will be an ongoing 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 current legislation.
- Detailed procedures are included in the Retention/ IT / School's Record Management Policy/Procedures.
- 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 containing sensitive information are cross-shredded if required. All electronic data will be removed by certified providers / appropriately trained staff using an approved method in the online safety 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 asset register.
- All disposals with a residual value up to £500 require the authorisation of the Headteacher, £500 and above is the full Governing Body

6.7.1 IT Asset Disposal and Personal Data Deletion Strategy

See School Data Protection and Information Security Policy, seek further guidance from the School's DPO.

- All information on computer hard drives 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 the Headteacher and the School Business Manager.
- 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 can be carried out for disposal of personal/sensitive information.
- See School Online Safety 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

See School Data Protection and Information Security Policy, seek further guidance from the School's DPO.

- There are acceptable use and online-safety policies for the internet and social media use that pupils/staff/visitors 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 Acceptable Use /Online Safety Policy is the responsibility of the online safety committee 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 online safety, the School is exploring the 360 degree Safer Online accreditation.
- 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 Acceptable Use policy could result in disciplinary action and/or sanctions.

7.2 Use of mobile Devices

See School Data Protection and Information Security Policy, seek further guidance from the School's DPO.

Mobile devices such as iPad 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 Online Safety Policy.

- Use of School staff 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 download School information to personal devices, e.g. Policies/Risk Assessments.
- 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 Online Safety Policy.
- 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.

The School is not used out of hours for non-School events or activities. The security risks associated with community use will be assessed by governors/trustees when reviewing future community use.

The School is not used for statutory purposes for polling or parish Council meetings.

- 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 can be alarm protected by use of the zoning facility of the alarm.
- The conditions of hire state that hirers should never vacate the premises before a member of staff has arrived to check and secure the building. A contact number is provided in case a hiring finishes before the expected time.
- Site Staff do not always remain on site during extended School's use and all out of hours use and hiring's but are contactable by phone.

- The Headteacher 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 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 School's EASEE Plan can be found in the School Main Office & with the Senior Leadership Team for full emergency procedures/contacts.

Police	In an emergency – 999 Non-emergency 101
Police Community Support Officer	02476 641111 Mailbox numbers: 16209, 16201
WES Safety and Premises	01926 412440 wespremises@warwickshire.gov.uk
Intruder alarm company details	Current Live 02476 228000 (Passcode: L11281) Out of Hours Dodd Group 0121 565 6012
Alarm Monitoring Company details@	Coventry Communications (Coventry City Council) 02476 832208 Emergency No: 02476 681369
CCTV company	N/A
Resources – Property Hotline	01926 414123
Insurance Details	WCC only Insurance Officer 01926 418160/412122 RPA 0330 058 5566

School Opening Hours

	Time	Time
Gates	Open from 6.00am	Close 7pm
Staff on site	In from 6.00am	Out 7pm
Children & families on site	In from 8.30am	Out 5pm
Hirings	N/A currently	N/A currently
Extended Services	8.30am	5pm

Appendix B School Property Marking Procedures

The School has chosen state marking product - chemical etching and/or chemical forensic marking (Smart Water) to protect equipment and property

1	Staff responsible for security marking Admin Staff Staff responsible for asset register/inventories School Business Manager/Admin Staff
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 £250 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	The School advertises the property marking system (as a deterrent) in the following way : window sticker

A written procedure is useful, noting who is responsible for the task, when it is done, e.g. prior to distribution. Marking could be tamper proof labels or Smart Water detailing the property name or postcode. Details can be included in the Security Policy. Further WES guidance on security marking products is available on the WES Website.