Eversley Primary School

Information Handling and Classification Policy

Author	**Steve Durbin**	Classification	**OFFICIAL**	Date of First Issue	**21/10/2017**
Owner	**IGB**	Issue Status	**FINAL**	Date of Latest Re-Issue	**29/01/2021**
Version	**1.4**	Page	**1 of 20**	Date of Next Review	**28/01/2022**
Reviewer	**Steve Durbin**			Date approved by Govenors	

CONTENTS

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

1. Aims of the Policy

1.1. Information is a valuable asset and aids a school to carry out its legal and statutory functions. The information that the our School processes can be highly confidential and very personal and therefore the School has a legal duty to take care of it. Like any other strategic asset, information must be protected appropriately depending on the level of sensitivity of the information.

1.2. The purpose of this document is to define the policies and standards that will be applied to maintain the confidentiality, integrity and availability of the information systems supporting the business functions of the School.

1.3. This policy provides direction and support for the implementation of information security and is designed to help the school workforce carryout the business of the School in a secure manner. By complying with this policy, the risks facing the School are minimised.

1.4. Anyone who uses the School's systems should be made aware of and be expected to comply with this policy and need to understand that the School has a responsibility to ensure that the school workforce must be cleared and trained to handle protectively-marked information.

1.5. The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the School Business Manager.

2. Scope and Definitions

2.1. This policy applies to all employees, contractors, agents and representatives and temporary staff working for or on behalf of the school.

2.2. The Policy is also applicable to Governors who create records in their capacity as representative of the School. When Governors create records when acting as representatives of the School they are recommended to apply the policy, but officers should consider whether it has been correctly applied on receipt of a governor's enquiry. It does not apply to those records the Board of Governors create when acting as a representative of a political party.

2.3. The above groups will be referred to as "**users**" for the remainder of this document.

2.4. Persons whose information is being used are referred to as "**data subjects**". A user can also be a data subject.

2.5. Partner organisations / third parties who access the School's information systems should also be aware of this policy and adhere to it when accessing School information systems.

2.6. This policy applies to all information created or held by the school, in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example IT system/database, network drive

folders, email, filing cabinet, shelving and personal filing drawers) as well as that communicated verbally. These will be referred to in this document as **Information Assets**. The persons responsible for managing, using or creating these will be designated as Information Asset Owners. All information assets must have an owner.

3. Other Considerations and References

3.1. The retention and disposal of information assets is in many instances a legal requirement, but we must also remember those that follow after us and decide what records must be kept for historians. This does not mean that all information must be retained forever, since the majority will not be looked at and we do not have the capacity to store it.

3.2. Responsibilities must therefore also be assigned to ensure that information assets are stored on a suitable medium and retained or destroyed in accordance with the School's Retention Schedule.

3.3. The following documents should be read in conjunction with this policy:

- Acceptable Use Policy
- Code of Conduct
- Data Protection Policy
- Freedom of Information Policy

4. Responsibilities under this policy

4.1. All users are responsible for:

- Adhering to School policies & processes
- Ensuring that they maintain the confidentiality of information assets disclosed to them as part of their duties
- Reporting information security incidents to the School Business Manager they become aware of, including those caused by themselves. The School operates a protected policy for reported information security incidents in a similar manner to whistleblowing policy.

4.2. All managers are responsible for:

- Authorising the publication of School data or information
- Approving exchange agreements with third parties
- Approving acceptable risks following risk assessment
- Authorising access to School information systems
- Reviewing access rights for users for whom they are responsible at least quarterly
- Ensuring that contingency plans and recovery procedures are in place to recover their business and operational processes

- Ensuring that their team members comply with the School's policies.

4.3. Information Asset owners and Authors are responsible for:

- Understanding what information is held and how it is used
- Determining the business requirements for the use of the information and signing them off
- Defining the classification/protective marking of the information asset
- Maintaining in conjunction with the School Business Manager the asset inventory including Data Protection Impact Assessments, risk registers for the information assets and all information required for compliance with the current data protection law.
- Specifying who has access - access may be given according to 'need to know' or role based
- Defining information sharing agreements and data interchange agreements
- Authorising changes in use of assets or the creation of new assets, following consultation with the Data Protection Officer whose advice must be recorded and, if disagreed with, reasons for disagreement recorded and justified
- Specifying back up and business continuity requirements
- Ensuring information is retained in accordance with policy and legislation
- Advising system administrators of access requirements
- Periodically reviewing users' access rights to ensure they meet business requirements, at least quarterly
- Ensuring information asset disposal is correctly carried out at the right times.
- Taking part in information asset and control audits

4.4. System administrators are responsible for:

- Managing / reviewing / analysing fault calls / issues
- Administering access to School information systems
- Reviewing / analysing system security logs
- Identifying information security breaches and weaknesses
- Ensuring that housekeeping, especially data backup schedules are in place and taken on a regular basis

4.5. The School Business Manager is responsible for:

- Managing / reviewing / analysing security breaches

- Reviewing / analysing network logs for potential / actual threats to information assets
- Maintaining threat intelligence and advising others on actions needed
- Raising with Governors areas of concern where they believe information asset handling could create threats to the council or data subjects.
- Acting upon reports of information security incidents.

5. Accountability for Assets

5.1. *All information and information assets will be identified, and an owner assigned. Owners of information assets may delegate their security authority (power to act) to individual user managers or service providers, but they remain ultimately accountable for ensuring that adequate security protection for the information assets s maintained*.

5.2. A list of information assets will be drawn up and maintained by Information Asset Owners and shared with School Business Manager who will keep the inventory for the school. This inventory must be accessible to all staff. The Information Asset Owners must update the inventory annually, and when any new data use is undertaken. The inventory should contain all information required by the data protection law This will ensure effective asset protection takes place and can be used by other business processes such as health and safety and for insurance purposes.

5.3. Information asset owners must be identified for each information asset used within the School. Accountability to an identified owner helps to ensure appropriate protection is maintained. The owner may delegate responsibility for the implementation of controls, however, accountability for the implementation of controls and their enforcement will stay with the owner at all times.

6. Legislation

6.1. The school workforce use School information systems must comply with all UK information legislation, particular the School's Data Protection Policy and be aware of any legislation pertinent to their own service area.

7. Confidentiality Agreements

7.1. All users will be required to sign that they have read and understood the School's Code of Conduct or a confidentiality / non-disclosure agreement prior to commencement of work with the School, dependent on status. These agreements identify the requirement for confidentiality whilst employed with the School, and include:

- A definition of the information to be protected (e.g. confidential information)

- Expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely
- Required actions when an agreement is terminated
- Responsibilities and actions of signatories to avoid unauthorised disclosure
- Ownership of information, intellectual property rights and how this relates to the protection of confidential information
- The permitted use of confidential information
- The right to audit and monitor activities that involve confidential information
- Process for notification and reporting of unauthorised disclosure or confidential information breaches
- Terms for information to be returned or destroyed and agreement cessation, and expected actions to be taken in case of a breach of agreement

8. Acceptable Use

8.1. To ensure that all information is protected, an Acceptable Use Policy has been established. All of the staff workforce are required to comply with this policy.

9. Documents and Records Management

9.1. Documents and records are another term for Information Assets.

9.2. There is a Documents and Records management policy giving high-level strategic goals which this policy implements.

10. Transmitting and Receiving Information Assets

10.1. Resources may be used to exchange information with customers and other third parties provided that:

- the risk has been assessed by School Business Manager and any significant change to the overall profile approved
- Any additional controls demanded by organisations under data sharing agreements are implemented.

10.2. The School must comply with relevant legislation and data sharing agreements when transmitting information. Where necessary, employees must:

- Not transmit data to 3rd parties without a valid Data Processing Agreement or Information Sharing Agreement.
- Ensure that any transmission containing such information includes the standard School disclaimer (automatically appended to outgoing e-mail)

11. Security of Information Assets Off Premises

11.1. Information assets which are held for home or mobile working or are transported away from normal work location must be carefully protected.

11.2. Home working controls should be determined by a risk assessment and suitable controls applied as appropriate. Adequate insurance cover should be in place to protect equipment off site. See also the School's Acceptable Use and BYOD Policies.

11.3. All reasonable precautions must be taken to safeguard School equipment and paper when outside the office.

11.4. Laptops, tablet devices, mobile phones and other portable devices storing data are vulnerable to theft, loss or unauthorised access when travelling. They should be provided with an appropriate form of access protection to prevent unauthorised access to their contents. Personal data at rest on such devices **must** be encrypted in accordance.

11.5. If it should become necessary to leave an information asset in an unattended vehicle, lock the asset securely in the boot or other storage space of the vehicle where it is not visible to passers-by.

11.6. Paper files must be carried in a way that does not allow others to read them (e.g. cover sheets), and should never be left unattended. If kept at home, this must be in a secure locked cabinet to which only school staff has access.

11.7. Devices in use in public spaces should have precautions to avoid information leakage via people reading over shoulders or via interception of Wi-Fi.

11.8. Any loss or theft of equipment or paper must be reported to the School Business Manager as soon as possible and in any case within 24 hours. Additionally, any theft should be report to the police and a crime reference number obtained. Please note that the legal reporting time to the information commissioner, which may be needed in some cases, is 72 hours, so schools should make arrangements for these issues to be recorded out of school hours.

12. Classification of information

12.1. **Introduction to classification**

12.1.1. Asset classification and control is an essential requirement, which will ensure the Confidentiality, Integrity and Availability of information used by the School. An information classification system is used to define appropriate protection levels and to communicate the need for special handling measures. Each information asset is classified to indicate its sensitivity and to identify the controls required to protect it.

12.1.2. The intention of the new classification to provide a more straightforward, proportionate and risk managed approach to the way that the school's classifies and protects information, with more onus on staff taking individual responsibility for the information they manage.

12.1.3. The school has adopted the Government's information classification policy which has one level of classification for all school information, with additional handling qualifiers for certain data.

12.1.4. The Government's classification scheme is widely used by government, local authorities and statutory agencies so that there is a common understanding across organisations as to how information needs to be protected.

12.2. **Classification Guidelines**

12.2.1. ALL information that the School needs to collect, store, process, generate or share to deliver services and conduct School business has intrinsic value and requires an appropriate degree of protection, whether in transit, at rest or whilst being processed.

12.2.2. Information classification or protective marking of information assets are used to:

- Determine the level of protection needed for the data
- Indicate that level of protection to other people
- Established a consistent approach to ensuring that data is appropriately protected.

12.2.3. Classification and protective information controls are established to meet with the School's need for sharing or restricting information. Information classification and their protective controls will be suited to the business need for sharing or restricting information and the business impact associated with such a need.

12.2.4. Classified data will be reviewed on a regular basis to assess if the security control is appropriate. The level of criticality of information assets will change due to changes in circumstances and / or expiry of legal retention periods.

12.3. The School's Classification Scheme

12.3.1. The School will only be using the OFFICIAL classification. However, the OFFICIAL classification also includes a handling caveat of OFFICIAL-SENSITIVE in order to identify information that should only be available on a strictly need to know basis and may need additional measures of protection. These classifications should be applied to all information including emails, paper documents, electronic documents, systems etc.

12.3.2. All School information will be classified as OFFICIAL unless there are specific handling requirements.

12.3.3. For OFFICIAL – SENSITIVE data common sense handling is required; extra care must be taken with storage and sharing. As this is a broad category and there will be variety of handling instructions associated with this information, the School is introducing sub-categories that give clear guidance on access arrangements for the information.

12.3.4. The complete list of protective markings and handling requirements for use is given below:

Classification Marking	Uses
OFFICIAL	Not covered under other categories and no special handling needed
OFFICIAL - SENSITIVE	Common sense handling required, extra care must be taken with storage and sharing. Encryption will be automatically applied externally on email.
OFFICIAL - SENSITIVE [PERSONAL]	As Official - Sensitive, contains information relating to individuals.
OFFICIAL - SENSITIVE [COMMERCIAL]	As Official - Sensitive, contains information with commercial implications.
OFFICIAL - SENSITIVE [GOVENORS]	As Official - Sensitive, contains information for Governors and involved officers only. Cannot be sent externally.
OFFICIAL - SENSITIVE [LEGAL]	As Official - Sensitive, contains information with sensitive legal advice.

12.3.5. Any information that is not marked will be assumed to be OFFICIAL.

12.3.6. The OFFICIAL-SENSITIVE caveat should be used at the discretion of staff depending on the subject area, context and any statutory or regulatory requirements where it is particularly important to enforce the need to know rules.

12.3.7. However, the caveat should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the 'need to know' as compromise or loss could have severe and damaging consequences for an individual (or group of individuals), another organisation or the School more generally. This might include, but is not limited to the following types of information:

- The most information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice on contentious and very sensitive issues;
- commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to the School or to a commercial partner if improperly accessed;

- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- more sensitive information about security assets or equipment that could damage capabilities or effectiveness;
- very sensitive personal data that would be extremely damaging to an individual if lost or compromised, e.g. child protection cases, HR compromise agreements,
- Government data where they have defined it as OFFICIAL-SENSITIVE and insist on strict sharing protocols

12.3.8. OFFICIAL-SENSITIVE data cannot be shared externally except through an approved secure email system / secure network or appropriate data encryption and password protection and should be accompanied by a defined distribution list. Data sharing with external organisations must be in line with school data sharing agreements or contract terms.

12.3.9. Where large volumes of OFFICIAL-SENSITIVE information about particular topics are regularly shared between organisations, the respective information asset owners will need to agree specific handling arrangements and transfer protocols in line with the policy.

12.3.10. A classification of OFFICIAL-SENSITIVE does not necessarily exempt the information from a Freedom of Information Act request but it should prompt you to consider if an exemption applies.

12.3.11. On creation, all information assets must be assessed and classified by the owner according to their content. All information assets must be classified and labelled in accordance with this policy.

12.4. **Information Labelling and Handling Procedure**

12.4.1. A set of procedures is defined for information labelling and handling in accordance with the classification scheme adopted by the School. All documents must be issued under version control with the file name and revision number and number of pages displayed in the footer. Where appropriate, the document will also contain its security classification and distribution list.

12.5. **Key Principles for all Protectively Marked material**

12.5.1. The key principles for protectively marked material are as follows:

- Access is granted on a genuine ‘need to know’ basis.
- Assets must be clearly and conspicuously marked. Where this is not practical (for example the asset is a building, computer etc.) staff must still have the appropriate personnel security control and be made aware of the protection and controls required.
- Only the author or designated information owner can protectively mark an asset. Any change to the protective marking requires the author or

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

information owner's permission. If they cannot be traced, a marking may be changed, but only by consensus with other key recipients.

- A file, or group of protectively marked documents or assets, must carry the protective marking of the **highest** marked document or asset contained within it (e.g. a file containing OFFICIAL and OFFICIAL - SENSITIVE material must be marked OFFICIAL - SENSITIVE).
- All data copied on removable media, (USB Flash memory, CD, etc.) must be encrypted; permission must be obtained from the information owner / author before copying and formally recorded e.g. via email.

12.6. Enforcement Monitoring

12.6.1. Monitoring of the policies is the responsibility of the School Business Manager as part of their management role. Internal and External Audit may undertake reviews on a planned and ad-hoc basis as part of the audit plan as agreed with the auditors.

12.7. Information Security Incidents

12.7.1. The School has a responsibility to monitor all incidents that occur within the organisation that may breach the security and/or the confidentiality of its information. All incidents need to be identified, reported, investigated and monitored. It is only by adopting this approach that the school can learn from its mistakes and prevent losses re-occurring.

12.7.2. The School has developed and implemented a Security Incident Response Policy, you should ensure that you read and understand both the policy and your responsibilities under the reporting process. In all cases you should follow the Security Incident Reporting Procedure.

12.7.3. The School also needs to take action where potential incidents are identified. Where 'near misses' occur, these should be reported to your School Business Manager and a local decision taken as to whether the cause of the 'near miss' is one which could involve the enhancement of the policy or the process. In all cases you should follow the Security Incident Reporting Procedure.

12.8. **Confidential Waste**

12.8.1. **Summary of handling requirements**

- Any Electronic Devices no longer required or faulty **must be returned to the school office.**
- **OFFICIAL-SENSITIVE paper material must be disposed of in confidential waste bags located in the main office or staffroom.**
- **Paper copies of OFFICIAL-SENSITIVE material to be disposed of through standard paper waste must be shredded using a cross-cut (dicing) shredder or placed in the confidential waste bins provided.** Shredders must cut to a maximum size of 5mm wide and 42mm long

- **Staff working from home** or at a place where confidential paper waste facilities are not available, should retain their paper waste and bring back to office for disposal as above
- **Document Management** shall store the documents securely and dispose of them with a registered waste carrier with secure destruction guarantees.

12.8.2. Paper Waste Handling

All paper documents including **MFD** (Multi Function Device) **jams** of blank paper, out of date **letterheads, printed forms,** can be placed in the recycle waste, on condition they are torn up, ensuring that they cannot later be removed and used inappropriately.

Paper confidential waste must be placed in either locked confidential waste bins or shredded and placed in paper recycling. Prior to placing in confidential waste bins, the paper must have all **staples, paper clips** and **binders** removed.

The use of shredders is permitted. Any shredders purchased should be **'cross cut'**, with a maximum shred size of 5mm x 42mm. Shredded paper should be placed in paper waste sacks for recycling disposal.

12.8.3. IT Waste Handling

Removable Media (memory sticks, CD's, DVD's, backup tapes)
Removable Media requiring disposal should be passed to IT. Staff must raise a call to arrange disposal

Other IT Equipment
The disposal of all other IT equipment e.g. PC's, printers is to be dealt with by IT.

Erasure Procedure for Disposal of IT Waste.
As there is no current UK standard for erasure following the deprecation of HMG Infosec standard 5, Media which is to be reused rather than destroyed should be erased following SP 800-88[1].

Note that older methods as specified by Infosec Standard 5 using multiple overwrites etc., are no longer applicable to modern technologies, especially solid state drives where wear levelling and relocation prevent complete erasure. This may present challenges with third parties using out of date policies, who may insist on inappropriate methods.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

Data that is regarded as OFFICIAL – SENSITIVE and not subject to other controls should be erased via CLEAR procedures. This should cover most data on School's systems. Where data shared with the School is subject to higher security requirements, general PURGE is sufficient.

Whilst reference needs to be made to the latest destruction requirements in FIPS SP 800-88, at the time of writing:

- Android and Windows phones, tablets with encryption for CLEAR – full factory reset performs a suitable Cryptographic Erase (CE). For PURGE destruction is recommended.
- iOS phones, tablets and unencrypted phones for CLEAR – manual erasure of all data followed by full factory reset. For PURGE destruction is recommended.
- Unencrypted ATA, SATA, NVM and SCSI drives for CLEAR and PURGE – use the built-in erase commands where supported and verify; if not supported single pass overwrite with zeros if drive is over 15Gb. Below 15Gb destruction is recommended for PURGE, two-pass overwrite with pattern and complement is recommended for drives <15
- Encrypted drives for CLEAR and PURGE – Cryptographic Erase (CE). Sanitised destruction of encryption keys.
  The process is as follows:
  - Manually enter the BIOS and clear the Trusted Platform Module (TPM)
  - Wipe the Recovery Key for the specific device from Active Directory (AD) and Microsoft BitLocker Administration and Monitoring (MBAM).

  Note: The School uses Microsoft BitLocker as a trustworthy technology (Latest status of NIST validation can be checked here Cryptographic Module Validation Program).

- USB Media, memory cards for CLEAR and PURGE – two-pass overwrite with pattern and complement.

For all completed cases of Clear, Purge or Destroy; appropriate evidence will be kept by school.

For any device or media type not mentioned above the minimum recommended sanitization techniques to Clear, Purge, or Destroy will follow the recommendation in Appendix A of SP 800-88.

13. Information Sharing Protocols

13.1. Before information is shared with other organisations, an information sharing protocol/exchange agreements between the School and the other organisation(s) should be in place. These agreements must include IT in their creation and be recorded in the Register of Information Sharing

Protocols maintained by the school as part of its data protection law compliance.

13.2. The Data Protection Officer must be consulted on all such protocols, and will advise on information management requirements within them.

14. E-mail

14.1. All e-mail sent to external organisations or individuals shall have a standard School disclaimer automatically attached to it. The disclaimer shall state that the information enclosed in the e-mail and any attachment(s) is for the designated recipient only and that access, reproduction, dissemination or use of the information by another other person is not permitted.

15. User Access Management

15.1. Individuals employed by or under contract to the School are granted access to all systems and resources that they require to fulfil their role. Employees not specifically granted access to School systems or resources are prohibited from using such systems or resources.

15.2. Access to data, systems or networks will only be granted to the school workforce that have formally agreed to comply with the School's information security policies. Only a system administrator may grant logical access to School systems and systems resources.

15.3. Periodically, all access rights must be reviewed and the School Business Manager will be required to formally check and amend the access rights of the school workforce.

16. Password Use

16.1. The school workforce must keep passwords confidential and:

16.2. Avoid keeping a written record of passwords

16.3. Request a password change whenever they believe their password has become compromised (this should also be reported as a potential security breach)

16.4. The sharing of User IDs and passwords is not permitted.

16.5. More detail on password management is provided in the Access Control Policy.

17. Unattended User Equipment

17.1. School workforce members are required to lock their devices (⊞+L on Windows machines, commonly power button on mobile devices) when they move away from their desk or are not using a device. This will require them to re-enter their password on return.

18. Legislative Requirements

18.1. Under no circumstances are employees allowed to engage in any activity that is illegal under local, national or international law while utilising School resources.

19. Clear Desk and Clear Screen Policy

19.1. Information must be protected at all times; unattended information assets must be secured. See the Acceptable Use Policy.

20. Third Party Access

20.1. Third parties requiring access to systems for any purpose are subject to additional controls.

21. Logging into/accessing Council systems

21.1. Each authorised user shall have a single unique user account that consists of:

- User name – a unique name
- Password – containing at least eight characters that includes letters (both upper case and lower case), numbers and special characters
- Preferably, a second authentication factor as described in the Access Control Policy

21.2. Only the assigned user may use that user ID to access School systems. Only users who have authenticated themselves to a School system may use that system.

21.3. All School systems where technically possible will display a security message to all people attempting to log-in in to that system that:

- access is restricted to authorised schools workforce only
- access to the system must comply with the School's Access Control Policy
- unauthorised access will be monitored and investigated.
- Once accessed, information systems should be used in line with the School's Acceptable Use Policy.

22. Reporting an Information Security Weakness, Threat, Event or Incident

22.1. The following example might be used to describe the difference between a weakness, threat, event or incident:

- A window with a broken latch is a weakness and poses a threat
- If an individual attempts to gain access through the window it is an event

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

- If the individual gains unauthorised access to confidential information through the window it is an incident (and has caused a breach).

22.2. It is vital that all such weaknesses, threats, events and incidents are reported immediately to IT, even if there is no adverse effect. Any observed or suspected security threats or weaknesses in systems or services should also be reported. If we do not know about them, they cannot be corrected.

22.3. Do not be afraid of reporting security issues – these are investigated with an appropriate degree of confidentiality. School workforce members who report near misses or incidents are also protected by the Whistle Blowing Policy.

22.4. The school workforce should not, in any circumstances, attempt to prove or validate a suspected information security weakness or threat, with the exception of IT.

23. Intellectual Property

23.1. The School owns all data, information and software design or code produced by or on behalf of the School, regardless of format, unless otherwise specified by a valid third party agreement.

23.2. All information or software developed by or on behalf of the School will remain the property of the School and must in no way be sold, copied or used without the express permission of the School or authorised designate.

23.3. All contracts with third parties, including contracts for agency employees, must define the ownership of software and information.

24. Software Licencing

24.1. Users are not generally permitted to install software on to the school network or School PCs, laptops or tablet devices.

24.2. For the purposes of definition, software includes but is not limited to any operating system, utility, programme, web service, cloud service, add-in or mobile application.

24.3. IT will maintain a register of the entire School's software and its location and must keep a library of software licenses.

24.4. Periodic software audits will be carried out by or on behalf of the school to ensure that all software loaded on to School information systems is appropriately licensed.

24.5. Commercial software may be installed or used on School computers only if a valid licence for that software has been purchased, and IT has recorded the use. IT are the only department allowed to purchase software.

25. Mobile Computing and Communications

25.1. It is the responsibility of school workforce members to take reasonable precautions to safeguard the security of all mobile equipment assigned to

them and the information contained upon them. Detailed security compliance is provided in the Acceptable Use Policy.

26. Remote Working

26.1. Remote Working (working at a site other than the usual place of work, e.g. another office location, home) is available to most of the school workforce at the School Business Manager's. They must follow the Acceptable Usage Policy.

27. Reporting of Malfunctions

27.1. If your system develops any software or hardware faults do not attempt to rectify it. You must report the malfunction to IT.

28. Removal of Property

28.1. School property shall not be removed from the premises without prior approval. Laptop and tablet device users are by default, allowed to remove their IT equipment from the premises.

28.2. **Removal/Disposal of Assets - Permanent**

28.3. The school workforce may not remove any commercial property or asset that is destined for destruction or disposal from School facilities, unless all the following conditions have been satisfied prior to removal of the property:

- A detailed list of the property concerned (including relevant serial, model and asset register numbers) is made on the appropriate property pass-out form, requesting the authority of the School Business Manager to remove it.
- IT makes enquiries to ensure the propriety of the request, and if satisfied signs the form, stating any necessary conditions. (e.g. 'Not for re-sale', or 'Must be degaussed prior to removal')
- The original copy of the form is to be lodged with IT. One copy is to be retained by the person removing the property and a further copy is to be passed to the School Business Manager to amend the asset register, where necessary.

28.4. **Removal/Disposal of Assets – Temporary**

28.4.1. School workforce members may not remove any commercial property or asset, on a temporary basis (i.e. to assist working from another location) from School facilities unless all the following

28.4.2. conditions have been satisfied prior to removal of the property:

- A detailed list of the property concerned (including relevant serial, model and asset register numbers) is made on the appropriate property pass-out form, requesting the authority of the School Business Manager to remove it.

- Prior to approval of the request, the School Business Manager should be satisfied of the necessity for the temporary removal and specify a date by which the asset must be returned to the School facility.
- The original copy of the form is to be lodged with the School Business Manager. One copy is to be retained by the person removing the property and a further copy is to be passed to IT in order that the asset register may be noted.
- The School Business Manager must notify the IT when the asset has been returned.

28.4.3. The above does not, of course, affect the accepted personal removal of issued laptops, tablets mobile telephones, pagers, paper files or the like for callout, home working or remote working purposes.

28.5. **Loss, Theft or Destruction of Assets**

28.5.1. The loss, theft or destruction of any School asset must be reported to the School Business Manager and IT as soon as is reasonably possible.

29. Policy Compliance

29.1. The School expects that all school workforce will achieve compliance to the directives presented within this policy. This policy will be included within the Information Security Internal Audit Programme, and compliance checks will take place to review the effectiveness of its implementation.

30. Exceptions

30.1. In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question.

- If complying with the policy would lead to physical harm or injury to a member of the school workforce
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises
- In such cases, school workforce members concerned must take the following action:
- Ensure that their manager is aware of the situation and the action to be taken
- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-conformance report
- Ensure that the situation is reported to the School Business Manager as soon as possible.
- Failure to take these steps may result in disciplinary action.

- In addition, IT maintains a list of known exceptions and non-conformities to the policy. This list contains:
- Known breaches that are in the process of being rectified
- Minor breaches that are not considered to be worth rectifying
- Any situations to which the policy is not considered applicable.

The School will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

31. Penalties

31.1. Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to the School or partner organisation
- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the School or partner organisation to actual or potential monetary loss through any compromise of security
- Any person who knows of or suspects a breach of this policy must report the facts immediately to the School Business Manager or Board of Governors.
- Any violation or non-compliance with this policy may be treated as serious misconduct.
- Penalties may include termination of employment or contractual arrangements, civil or criminal prosecution.