THE PIGGOTT SCHOOL

'Go and do Likewise' Luke 10:25-37, The Parable of the Good Samaritan
We live with love and compassion, seeking help in times of need

INFORMATION SECURITY GUIDELINES POLICY

Date last reviewed:	January 2020
Responsibility:	Headteacher, Data Protection Officer and SALT Committee
Review Period:	Annually
Data Protection Officer:	David Thatcher

Contents

1. Introduction

1.1 All personal information held by the school, in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.

1.2 This policy is in two parts, the first outlines security procedures covering all aspects of processing information. The second part covers security of IT systems.

1.3 The policy must be read in conjunction with other Information Management and IT Policies, including

- Acceptable use Policy
- Internet access Policy

1.4 The policy applies to all employees of the school, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by the school, but engaged to work with or who have access to the schools information, (e.g. computer maintenance contractors, supply teachers, PGCE etc) and in respect of any externally hosted computer systems.

1.5 The policy applies to all locations from which school systems are accessed (including home use). Where there are links to enable non-school organisations to have access to information, staff must confirm the security policies they operate meet the schools security requirements. A copy of any relevant third party security policy should be obtained and retained with the contract or agreement.

1.6 Suitable third party processing agreements must be in place before any third party is allowed access to personal information for which the school is responsible.

2 Policy Compliance

2.1 All staff are expected to be aware of and understand the content of this policy.

2.2 If any staff member is found to have breached this policy, they could be subject to school's disciplinary and grievance policy & procedure. Serious breaches of this policy could be regarded as gross misconduct.

3 Legal Aspects

3.1 Some aspects of information security are governed by legislation, the most notable UK Acts and European legislation are listed below. Further information on each can be found in Appendix 2:

- The Data Protection Act (2018)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- General Data Protection Regulations (GDPR)

4 Responsibilities

4.1 Line Managers must:

- be aware of information or portable ICT equipment which is removed from the school for the purpose of site visits or home working and ensure staff are aware of the security requirements detailed in section 9, below
- ensure all staff, whether permanent or temporary, are instructed in their security responsibilities
- ensure staff using computer systems/media are trained in their use – the IT support department will assist with the induction and training of IT use in the school.
- determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status
- ensure staff are unable to gain unauthorised access to IT systems or manual data
- implement procedures to minimise the schools exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas
- ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable.
- ensure that the school's IT support staff are advised immediately about staff changes affecting computer access (e.g. job function changes leaving department or the school) so that accounts and mailing lists may be withdrawn or changed as appropriate.
- Ensure all relevant staff are aware of and comply with any restrictions.

4.2 All members of staff are responsible for:

- ensuring that no breaches of information security result from their actions
- reporting any breach, or suspected breach of security without delay. (Information relating to breach reporting can be found in the Data Breach Notification Policy)
- ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from any potential loss. Ensuring they are aware of and comply with any restrictions specific to their role or service area.

4.3 Advice and guidance on information security can be provided by Data Protection Officer and, in relation to IT security, the IT Manager.

5 PART 1 - KEEPING INFORMATION SECURE

6 Privacy by Design

6.1 Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The General Data Protection Regulations (GDPR) introduces a legal requirement for privacy impact assessments and privacy by design in certain

circumstances.

6.2 The school will, therefore, ensure that privacy and data protection is a key consideration in the early stages of any central IT project, and then throughout its lifecycle. A comprehensive Data Protection Impact Assessment (DPIA) would be carried out for any such projects

Projects may include:

- A new IT system for storing and accessing personal information
- A new data sharing initiative
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- Introduction of a new surveillance system (CCTV) or the application of new technology to an existing system.

6.3 Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Legal obligations are met and data breaches are minimised
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

7 Data Breaches and Information Security Incidents

7.1 The school has a duty to ensure that all personal information is processed in compliance with the principles set out in the Data Protection Act. It is ultimately the responsibility of each member of staff to ensure that they comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information. Information relating to breach reporting can be found in the Data Breach Notification Policy.

7.2 The Data Protection Principles can be found Here -

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

7.3 The GDPR requires the School to take

'appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'

7.4 A data breach could be defined as the unintentional release of personal or sensitive personal information to an unauthorised person, either through accidental disclosure or loss/theft. However, non-compliance with any of the 8 Data Protection Principles could be classed as a breach, particularly if there is a possibility that the person could be put at risk or suffer substantial damage or distress. This could relate to, for example, decisions taken based on inaccurate information (the 4th Principle).

7.5 A security incident is defined as a breach of school security which may result in a risk of loss, access to or corruption of school information or assets, whether personal or not. Examples of data breaches and security incidents, including the reporting process, can be found at Appendix 1.

7.6 In the event of any breach or security incident, it is vital that action is taken to minimise any associated risk to either the school or its customers as soon as possible.

7.7 It is important that all staff are aware of their responsibilities when handling personal information, keeping it secure and not disclosing it without proper cause. Suitable information handling procedures should be in place and all staff must undertake mandatory Data Protection training on an annual basis.

7.8 Similarly, staff must be alert to the possibility of cyber-attacks or phishing attempts. Further information on cyber security can be found at Appendix 4.

8 Access control

8.1 Staff members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation.

8.2 Formal procedures will be used to control access to systems. An authorised manager must raise an IT Service Request for each application for access to something that is presently not available to a computer user. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise IT Support of any changes requiring such modification/removal.

8.3 Staff members and contractors must comply with the schools 'Acceptable Usage Internet Policy' in relation to passwords.

8.4 When a member of staff leaves the employment of the school the IT Staff must be informed and all equipment loaned to the staff member must be returned before the end of their contract.

8.5 Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

8.6 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

8.7 The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment.

8.8 Once an employee has left, it can be impossible to enforce security disciplines, even through legal processes. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

8.9 System administrators will delete or disable all identification codes and passwords relating to members of staff who leave the employment of the school on their last working day. The employee's manager should ensure that all PC files of continuing interest to the business of the school are transferred to another user before the member of staff leaves.

8.10 Prior to an office staff member leaving, it is good practice for a meeting to be held during which the manager notes all the systems to which the member of staff had access and

informs the relevant system administrators of the leaving date. Special care needs to be taken when access to personal, commercially sensitive or financial data is involved.

8.11 Managers must ensure that staff leaving the schools employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then IT should be informed so that access rights can be restricted to avoid damage to information and equipment.

8.12 All visitors should have official identification issued by the school. If temporary ID or passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

8.13 There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. IT Services will advise on the most suitable control.

8.14 Staff should challenge strangers on site without an ID badge.

9 Security of Equipment

9.1 Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

9.2 Computer equipment is vulnerable to theft, loss or unauthorised access. Always use ⊞ + L keys on the keyboard to secure computers when leaving a classroom/office unattended and lock portable equipment away when you are leaving the office.

9.3 Due to car thefts, laptops or other portable equipment must **never** be left unattended in cars. Well-equipped thieves use technology to find cars with wireless devices left in them.

9.4 Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off school property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

9.5 Staff working from home must ensure appropriate security is in place to protect equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring equipment and information is kept out of sight.

9.6 School issued equipment must not be used by non-school staff.

9.7 All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the school.

9.8 Users of portable equipment away from school premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

9.9 Staff and members who use portable computers belonging to the school must use them solely for school purposes.

10 Payment Card Industry (PCI) Compliance

10.1 The school is currently PCI DSS compliant. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that

process, store or transmit credit or debit card information maintain a secure environment.

10.2 Failure to comply with these standards could lead to fines or even the removal of the school's ability to accept card payments.

10.3 Those users who have access to any part of the school's Cash/Payment Systems whereby they are taking payments either in person or over the phone should only take Cash/Cheque. We have online systems to negate the need for credit cards information to ever get to the school. **Under no circumstances** should card holder data such as card numbers be written down or copied by anybody as this would breach our PCI compliance.

11 Security and Storage of Information

11.1 All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to Office based IT systems
- Computer screens to be 'locked' (⊞ + L) whenever staff leave their desk
- Removable media (CDs/Memory Sticks) to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must **never** be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through the school's network.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

12 Posting, Emailing or Faxing Information

12.1 If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

12.2 Please consider the risk of harm or distress that could be caused to the customer if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

12.3 It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

12.4 Sending information by fax:

- telephone ahead to advise the fax is being sent and ask for confirmation of receipt
- Check the fax number is correct and dial carefully
- If the information is particularly sensitive, send a test fax to ensure it reaches the correct recipient
- Always use a fax header sheet, with contact details of sender and recipient

12.5 Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password eg telephone call, messenger or text.
- Consider the use of secure email where this is available
- Person identifiable data files **must not** be sent via email to a user's personal mail box. Staff working from home should only access information via the Schools Remote Apps/Office 365/Google apps systems.

12.6 Sending information by post:

- Check that the address is correct
- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error
- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the post room, this could be by recorded, special delivery or even courier.

12.7 Printing and Photocopying:

- All printing must be via the school copiers/printers to maintain an audit trail of information printed
- Consideration must be given to using the print room for large print runs, especially where personal information is concerned
- When printing or photocopying multiple documents, ensure you separate them when you return to your desk
- If the copier jams please remove all documents – if the copier remains jammed report it. If possible, cancel your print run.

- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run

- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

13 Redacting

13.1 If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used

13.2 The use of black marker pen is **not** a suitable method of redaction

13.3 It is not advisable to change the colour of text (eg white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

14 Sharing and Disclosing Information

14.1 When disclosing personal or sensitive information to anyone, particularly over the phone or in person, ensure you verify their identity. People dealing with parents or contractors on a daily basis should have suitable security questions which must always be used. If in doubt ask for suitable ID or offer to post the information (to the contact details you have on file)

14.2 If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf

- verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

14.3 In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

15 Retention and Disposal of Information

15.1 Information must only be retained for as long as it is needed for business purposes, or in accordance with the schools' retention periods

15.2 The school has adopted the guidance set out in the 'Information and Records Management Society Toolkit for Schools version 5'. This sets out the type of information held in the school, together with statutory or agreed retention periods. Please contact the Data Protection Officer for further advice on retention

15.3 When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins or shredding. Electronic information must be permanently destroyed.

15.4 When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage

15.5 All information destroyed in accordance with the retention periods must be logged on the Disposal Log

16 Vacating Premises or Disposing of Equipment

16.1 It is important that a process is in place to ensure all personal information is removed from premises should they be vacated, and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

16.2 The disposal of computer or other electronic devices is referenced in Section 27 of this policy and all electronic equipment must be returned to IT to be properly disposed of.

16.3 If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

16.4 Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers. If a cupboard or cabinet is locked and no key is available, Caretakers should be asked to open it in order that it can be checked.

17 PART 2 – IT SECURITY

18 Cloud Storage Solutions

18.1 The use of cloud storage solutions (SkyDrive, Onedrive Personal, iCloud etc.) for the transfer of school information is expressly forbidden. IT services have provided you with access to the schools secure Onedrive for Business for the sharing of files with home systems, pupils and other staff.

19 Systems Development

19.1 All system developments must comply with the school's IT Strategy. All system developments must take into account security issues in their consideration of new developments, seeking guidance from the IT Manager and performing an Internal Audit, where appropriate.

20 Network Security

20.1 The school's IT support Staff routinely review the security of the schools' IT Systems and will take action to maintain security of the data held within.

21 Phishing Emails

21.1 From time to time you may get an email requesting you to log into a website or to open an attachment that then asks you to log in to open it. These are usually an attempt to obtain your login details and should be ignored/deleted.

21.2 Our systems will not ask you to log in via email messages. Please do not comply with any such requests to sign in to confirm your identity especially if you don't recognise the sender or think the message out of the norm**.**
If unsure please contact the IT Systems Manager on 221 or technical@piggottschool.org

22 Risks from Viruses

22.1 Viruses (including malware and zero day threats) are one of the greatest threats to the schools 'computer systems. PC viruses become easier to avoid with staff and members aware of the risks with unlicensed software or bringing data/software from outside the school on a memory stick. Anti-virus measures reduce the risks of damage to the network and is maintained and monitored by the IT Support Team.

22.2 IT Support centrally maintains and updates the virus definition files on servers, Laptops and desktop PCs, but users are responsible for checking that virus updates are automatically occurring on all personal desktop machines at home.

Advice and support is available from IT Support if any remedial action is necessary. Any suspected virus attacks must be reported to technical@piggottschool.org

22.3 Anti-virus guidelines can be found at Appendix 3.

23 Cyber Security

23.1 Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of the school.

23.2 The school's approach to cyber security can be found in Appendix 4.

24 Access Control to Secure Areas

24.1 Secure areas include:

- The Exams storage room
- Main School Office
- The ICT server rooms (room11, KS4 office and 6th form)

24.2 All central processors/networked file servers/central network equipment will be located in secure areas with restricted access.

24.3 Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked cabinets.

24.4 Unrestricted access to the office computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.

24.5 Representatives of third party support agencies will only be given access through specific authorisation or accompaniment.

25 Security of Third Party Access

25.1 No external agency will be given access to any of the schools' curriculum or office networks unless that body has been formally authorised to have access.

25.2 All visiting external agencies will be required to sign in at reception.

25.3 All external agencies processing personal information on the schools' behalf will be required to provide a written statement regarding their GDPR Compliance.

25.4 The school will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

25.5 The school will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

25.6 All third parties and any outsourced operations will be liable to the same level of confidentiality as school staff.

26 Data Back-up

26.1 Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive without the approval of the IT Manager.

26.2 Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

26.3 IT Services and all other systems administrators should produce written backup instructions for each system under their management. The backup copies should be clearly labelled and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up. A cyclical system, whereby several generations of backup are kept, is in operation.

26.4 Archived and recovery data should be accorded the same security as live data and should be held separately from the servers. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The school's retention schedule must be followed in determining whether data should be archived.

26.5 Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

26.6 To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

26.7 Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

26.8 If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

27 Equipment, Media and Data Disposal

27.1 If a machine has ever been used to process personal data as defined under the Data Protection Act (2018) or 'in confidence' data, then any storage media should be disposed of

only after reliable precautions to destroy the data have been taken.

27.2 Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

27.3 Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using commonly available utility software. Therefore, disposal must be arranged through IT Services who will arrange for disks to be wiped or destroyed to the appropriate standards.

28 Software

28.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. You should retain a copy of the licensing information for any software you have asked IT to install outside of the normal PC build provided by IT services.

28.2 The loading and use of unlicensed software on school computing equipment is **NOT** allowed. All staff and members must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The school monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the school's disciplinary and grievance policy & procedures.

28.3 The school will only permit authorised software to be installed on its PCs. Approval will be via IT Services.

28.4 Where the school recognises the need for specific specialised PC products, such products should be registered with IT Services and be fully licensed.

28.5 Software packages must comply with and not compromise school security standards.

28.6 Computers owned by the school are only to be used for the work of the school. The copying of leisure software on to computing equipment owned by the school is not allowed. Copying of leisure software may result in disciplinary action under the school's disciplinary and grievance policy & procedures. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

28.7 Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by IT Services staff or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

28.8 The school seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to IT Services. See appendix 3 for the anti-virus guidelines.

28.9 Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact IT Services for anti-virus advice.

29 Use of Removable Media

29.1 It is the school's policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid case for its use is approved. Secure memory sticks are available from the IT support office on request.

29.2 All staff, members and third parties must comply with the requirements regarding removable media which can be found in the internet access policy.

30 Timeout Procedures

30.1 Inactive computers are set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. In high risk areas the time-out facility should also lock the computer. A high risk area might be an office with a windows giving access to the computer screen, or an unlockable area such as reception.

30.2 Users must 'lock' their computers (⊞ + L) , if leaving them unattended for any length of time.

31 System Documentation

31.1 All systems should be adequately documented by the IT Manager and should be kept up to date so that it matches the state of the system at all times.

31.2 System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

31.3 Distribution of system documentation should be formally authorised by the system manager. System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.

31.4 General Internet access carries with it a security risk of downloading viruses or programs that can look around a network and infiltrate password security systems. This information can then be sent back to the originator of the program in order to allow them unauthorised access to our systems. Therefore care must be taken when transferring data between your home PC and the School network. All home PCs which are used for the manipulation of School data must have a current virus checker with up to date virus signatures.

APPENDIX 1 - Reporting Data Breaches and Information Security Incidents

Reporting Data Breaches and Security Incidents

All employees, elected members, contractors and the schools' business partners have a responsibility to report any security incidents without delay. Staff should refer to the school's 'GDPR Data Protection Policy' and 'Data Breach Notification Policy' for more information on breach reporting.

A security incident is any event which has caused or has the potential to cause damage to the school's information assets. A data breach is the loss or release of personal information as a result of a security incident. Security incidents will include:

- Unauthorised persons gaining or seeking to gain access to school premises
- Unauthorised persons gaining or seeking to gain access to the school's information systems whether operated by or on behalf of the School
- Loss, theft, misuse, damage or destruction of any school information asset or equipment
- Computer virus import or infection
- Loss or theft of hard copy documents containing personal information
- Unforeseen incidents such as flood or fire
- Hacking attacks
- Use of media in school machines that have not been virus checked
- Failure to make adequate arrangements for information backup
- Unauthorised copying, amendment or deletion of data or software
- Unauthorised copying or use of access security cards
- Unauthorised disclosure or use of passwords, data or software
- Alteration, falsification or tampering with audit records or evidence
- Unauthorised monitoring of information systems, employees, members or business partners
- Use of the internet in contravention of UK law and the School's 'Acceptable Internet Usage Policy'
- 'blagging' offences where information is obtained by deception
- Information being disclosed inappropriately, for example, to unintended recipients or published on a website

Failure to report a security incident could lead to disciplinary action. Incidents that might constitute a breach of the security policy can be reported by following the procedure below or by using the school's whistleblowing policy.

It is also a criminal offence under the Data Protection Act for an individual to:

- Unlawfully obtain, disclose or procure the disclosure of personal information

- Sell or offer to sell personal information which has been unlawfully obtained

Upon discovery or suspicion of a security incident, a written record should be created, to include:

- date, time and location of incident
- nature of the incident, including any apparent loss
- if possible, the identity of any involved persons and witnesses
- details of the information assets affected.

Staff must not place themselves in any danger - personal security is more important.

All IT security incidents or suspected incidents must be reported immediately to the IT Manager on extension 221 or by email to technical@piggottschool.org

All incidents that result in the unauthorised disclosure of personal data must also be reported to the Data Protection Officer on extension 303 or by email to DPO@piggottschool.org

APPENDIX 2 - Legal Requirements Data Protection Act 2018

The processing of personal information must comply with the Data Protection Act 2018

The Data Protection Act states that 'when carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest..'

The Information Commissioner has the power to issue a monetary penalty for an infringement of the provisions of Part 3 of the Act – Law Enforcement Processing. Any penalty that we issue is intended to be effective, proportionate and dissuasive, and will be decided on a case by case basis.

Under Part 6 of the Act, there are two tiers of penalty for an infringement of Part 3 - the higher maximum and the standard maximum.

What is the higher maximum?
The higher maximum amount, is 20 million Euros (or equivalent in sterling) or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

What is the standard maximum?
If there is an infringement of other provisions, such as administrative requirements of the legislation, the standard maximum amount will apply, which is 10 million Euros (or equivalent in sterling) or 2% of the total annual worldwide turnover in the preceding financial year, whichever is higher.

The Data Protection Act 2018 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

Copyright, Designs and Patents Act 1988

This Act states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired.

Each manager is responsible for ensuring that all items of software in their business unit are either purchased through, or sanctioned by, IT Services.

All software purchased will have an appropriate licence agreement which may or may not be a site-wide licence. The School, through IT Services, will carry out periodic spot checks to ensure compliance with Copyright Law. Any infringement or breach of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the school's Disciplinary and grievance policy & procedure.

Computer Misuse Act 1990

This Act states that it is a criminal offence to attempt to gain access to computer information for which you have no authorisation. If it is suspected that any unauthorised access is made to a computer system then disciplinary action may be taken under the school's Disciplinary and grievance policy & procedure.

On ending their employment or work for the school, employees and contractors must not disclose information which was confidential.

GDPR

New Global Data Protection Laws affect all public bodies and businesses that hold personal information about the public and their staff.

Information about the details of GDPR can be obtained on the GDPR legislation website

APPENDIX 3 - Anti-Virus Guidelines

1. What is a virus?

A computer virus is a damaging piece of software that can be transferred between programs or between computers without the knowledge of the user. When the virus software is activated (by incorporated instructions, e.g. on a particular date), it performs a range of actions such as displaying a message, corrupting software, files and data to make them unusable, and deleting files and/or data. While many of the viruses produced are benign and cause no real damage to the infected system, they always constitute a breach of security.

There are currently something like 60-75,000 known viruses and worms [1] - some 10-20 new viruses or variants appear a day. When a virus or worm is released into the public domain, network worms and mass mailer viruses can sometimes spread worldwide before anti-virus vendors have had time to produce updates.

Even daily anti-virus updates are not always enough to ensure safety from all possible threats.

2. What does the school's IT Services do to prevent the spread of viruses?

Whilst precautions are taken at the network level to minimise the spread and impact of worms and viruses, it is not possible to make the process totally effective. Protection from viruses and worms is not a process that can be left entirely to system administrators, security officers, and anti-virus software. The best efforts of administrators and security experts are not sufficient - all computer users must also play their part by taking simple precautions like those described below.

3. Avoid Unauthorised Software

Programs like games, joke programs, cute screensavers, unauthorised utility programs and so on can sometimes be the source of difficulties even if they are genuinely non-malicious. That is why it is forbidden to install them. If such programs are claimed to be some form of antivirus or anti-Trojan [2] utility, there is a high risk that they are actually in some way malicious!

A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

[1] In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

4. Treat all attachments with caution

It makes sense to be cautious about email attachments from people you don't know. However, if attachments are sent to you by someone you do know, don't assume they must be OK because you trust the sender.

Worms generally spread by sending themselves without the knowledge of the person from whose account they spread. If you do not know the sender or are not expecting any messages from the sender about that topic, it is worth checking with the sender that they intended to send a message, and if so, whether they intended to include any attachment. If you were expecting an attachment from them, this may not apply.

However, one recent virus sends out an email telling you that a 'safe' attachment is on the way, then sends out mail with a copy of itself as an attachment.

Bear in mind that even legitimate, expected attachments can be virus infected: worms and viruses are related, but cause slightly different problems.

Regard anything that meets the following criteria with particular suspicion:

If they come from someone you don't know, who has no legitimate reason to send them to you.

- If an attachment arrives with an empty message.
- If there is some text in the message, but it doesn't mention the attachment.
- If there is a message, but it doesn't seem to make sense.
- If there is a message, but it seems uncharacteristic of the sender (either in its content or in the way it's expressed).
- If it concerns unusual material like pornographic web-sites, erotic pictures and so on.
- If the message doesn't include any personal references at all, (for instance a short message that just says something like "You must take a look at this", or "I'm sending you this because I need your advice" or "I love you!").
- the attachment has a filename extension that indicates a program file (such as those listed below).
- If it has a filename with a 'double extension', like FILENAME.JPG.vbs or FILENAME.TXT.scr, that may be extremely suspicious. As far as Windows is concerned, it's the last part of the name that counts, so check that against the list below to find out whether it's a program like those listed, masquerading as a data file, such as a text file or JPEG (graphics) file.
- In all the above instances, it is recommended that you check with the sender that they knowingly sent the mail/attachment in question.

5. Avoid unnecessary macros

If Word or Excel warn you that a document you're in the process of opening contains macros, regard the document with particular suspicion unless you are expecting the document and you know that it's supposed to contain macros.

Even then, don't enable macros if you don't need to. It may be worth checking with the person who sent it to you that it is supposed to contain macros.

6. Be cautious with encrypted files

If you receive an encrypted (passworded) attachment, it will normally be legitimate mail from someone you know, sent intentionally (though the sender is unlikely to know in the event that they have a virus). However, that doesn't necessarily mean that it isn't virus-infected. If it started out infected, encryption won't fix it. Furthermore, encrypted attachments can't usually be scanned for viruses in transit: the onus is on the recipient to be sure the decrypted file is checked before it's opened. This goes not only for heavyweight encryption packages, but also for files compressed and encrypted with PKZip or WinZip.

7. Suspicious filename extensions

The following is a list of filename extensions that indicate an executable program, or a data file that can contain executable programs in the form of macros. This list is by no means all-inclusive. There are probably a couple of hundred filename extensions that denote an executable program of some sort.

Furthermore, there are filenames like .RTF that shouldn't include program content, but sometimes can, while Word documents (for instance) can in principle have any filename extension, or none. Furthermore, zipped (compressed) files with the filename extension .ZIP can contain one or more of any kind of file.

.BAT	.CHM	.CMD	.COM	.DLL	.DOC	.DOT
.EXE	.FON	.HTA	.JS	.OVL	.PIF	.SCR
.SHB	.SHS	.VBS	.VBA	.WIZ	.XLA	.XLS

8. Report it!

If you think that you may have received a virus - report it!

In Microsoft Word and other programs, a macro is a saved sequence of commands or keyboard strokes that can be stored and then recalled with a single command or keyboard stroke. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it.

APPENDIX 4 - Cyber Security Approach

1. Cyber Security Introduction

This document identifies the risks to the school from main threats of cyber security and sets out what is in place to mitigate these risks.

If you do not understand anything in this document or feel you need specific training you should bring this to the attention of your line manager.

2. Purpose and Objectives

The document provides guidance to staff and members on the risks that threats from cyber security pose to the school.

In addition the following policies are relevant to all staff and have some impact on the threats from cyber security:

- Network Use Policy
- Acceptable use Policy

3. Roles and Responsibilities

The IT Manager is responsible for the provision of the appropriate technology and technological devices to ensure that the school is reasonably protected from the threats from cyber security.

The school is responsible ensuring that staff are communicated with about how to ensure that they don't put the School at risk.

All employees, contractors and members should not take any action that puts the schools' systems or information at risk from cyber security. Any incidents must be reported in line with the Information Security policy.

4. Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the school, the delivery of local public services and ultimately have the potential to compromise national security. Additional costs will be incurred by the school to rectify any cyber security or cybercrime event.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

The scale of targeted attacks, coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Foreign states, criminals, hacktivists, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- Stealing sensitive information to gain economic, diplomatic or military advantage over the UK
- Financial gain
- Attracting publicity for a political cause
- Embarrassing central and local government
- Controlling computer infrastructure to support other nefarious activity
- Disrupting or destroying computer infrastructure School employees

  can also be targets for criminal activity.

5. Cyber Security Risks

The following types of cyber security all pose risks to the school:

Cybercrime:

The most common form of cyber-attack against public bodies is the use of stolen or false customer credentials to commit fraud.

The uptake in online services means this form of crime can now be undertaken on a much larger scale and can be international.

Cybercriminals also seek to steal data from government networks that has a value on the black market, such as financial information or data that can be used for ID theft.

There are several types of malware (malicious software) that have been written to specifically steal banking and log in information.

The school secures its network with up to date antivirus and malware protection, and manages the use of personal USB devices on school computers.

Hacktivism:

Hacktivists seek to cause embarrassment or annoyance to the owners of high- profile websites and social media platforms that they may deface or take off line.

When targeted against local government websites and networks, these attacks can cause reputational harm both locally and nationally.

The school has third party availability monitoring tools in place to alert key team members of the websites status.

The school's web site's content management system conforms to the school's ICT Policy with regards to password enforcement.

Insider threats:

An insider is someone who exploits, or intends to exploit, their legitimate access to an organisation's assets for unauthorised purposes. Such activity can include:

- Unauthorised disclosure of sensitive information

- Facilitation of third party access to an organisation's assets
- Physical sabotage
- Electronic or IT sabotage

Not all insiders deliberately set out to betray their organisation. An unwitting insider may compromise their organisation through poor judgment or due to a lack of understanding of security procedures.

The insider threat is not new, but the environment in which insiders operate has changed significantly. Technology advances have created opportunities for staff at all levels to access information.

The school enforces the use of strong passwords for access to systems.

The school only allows corporate USB devices to be written to. All personal USB devices are read only.

The school uses mobile device management tools to secure corporate information on personal devices (smart phones and tablets).

The school periodically reviews access to key IT systems.

Physical Threats:

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster natural or otherwise that could impact upon local government IT systems.

The school has a disaster recovery (DR) and business continuity (BC) data centre for its high impact services. It also has a shared telephony platform with Hart District School with DR / BC built in.

Terrorists:

Some terrorist groups demonstrate intent to conduct cyber-attacks, but have limited technical capability. Terrorist groups could acquire improved capability in a number of ways, namely through the sharing of expertise in online forums providing an opportunity for escalations and the hiring of Hacktivists.

The school's approach to Cyber Security

As with most local authorities, the School relies heavily on access to the internet and to information held in its systems. There are several IT systems that have an internet presence (website, webmail homeworking), and there are several different access mechanisms to information (Wi-Fi, physical networking, smartphones, tablets). All present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but the school employs a range of tools and good practice to minimise the risk to its information and systems.

The school has clear polices on ICT and Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Passwords
- Removable Media
- Clear desk policy
- Sharing and disclosing information
- Cloud storage systems

- Viruses
- Equipment, media and data disposal

The school implements security controls and good practice to enable it to achieve compliance with Payment Card Industry Data Security Standards (PCI DSS) and Public Services Network (PSN). Both of these require the School to ensure that systems are security patched and that the School has regular tests of its network/systems that are performed by the IT Manager.

The school employs a range of technologies and processes to help it achieve a good security platform. These range from up to date firewalls and core networking equipment, through antivirus controls and a secure wireless configuration, to encrypted devices, two factor authentication and basic mobile device management.

6. Communications-Electronic Security Group (CESG)

CESG is part of GCHQ and provide assistance to government departments on information security and assurance.

CESG has published a document detailing 10 Steps to Cyber Security, these are listed below along with the steps that the School has adopted to mitigate the risks.

Information Risk Management Regime. The information governance team manages information risk proactively through the school's Information Management Policy which provides information to staff and members about information retention and disposal and information sharing. The team works with service areas to help them design and implement regimes for their information.

Secure Configuration. The school's IT service has default build processes for corporate devices and ensures that operating systems, services and applications are patched against known vulnerabilities. All corporate computers and servers are inventoried. Servers and network environments log activities for auditing purposes.

Network Security. The IT service manages a number of tools sets to ensure network security; these are periodically reviewed to ensure they meet security and business needs. The security configuration is also reviewed annually as part of the school's PSN submission. Internal and external network access is regularly tested by third party security consultants.

Managing User Privileges. The IT service manages core systems and applications. User logins for computers are managed by the IT service and access to information must be requested by a manager through an IT Service Request. Access to corporate applications is managed by the IT service and permissions granted in line with job requirements. Wherever possible user activity is logged, access to activity logs is restricted to IT System Administrators and Internal Audit.

User Education and Awareness. The IT service and the Information Governance team periodically send emails and information about threats to the organisation.

Policies and mandatory eLearning are in place.

Incident Management. The school has processes and recovery places for disaster recovery and business continuity. These are managed by the IT service and collated centrally within the Finance and Resources Directorate. There are also processes in place for the reporting and response for information and security incidents.

Malware prevention. The IT Service manages the School's antivirus and malware solutions. Signatures for malware and antivirus are updated automatically on all corporate computers.

Monitoring. The IT Service logs all system and security events across its server environment, and has software in place to alert for internal and external threat attempts. The school subscribes to Cybersecurity information Sharing Partnership (CiSP) for third party alerting and expertise.

Removable Media Controls. The IT service has implemented a solution to manage USB devices on corporate devices, ensuring that only approved and encrypted devices can be written to. Presently this is relaxed to a monitoring-only solution during the transition to cloud based personal storage.

Home and Mobile working. The IT Service employs a number of tools to ensure security of

information for home and mobile working, including Mobile Device Management solutions to encrypt School mobile devices and information on personal devices.

Information transported over virtual private networks (VPN's) is encrypted.