CRUDGINGTON PRIMARY SCHOOL INFORMATION SECURITY POLICY

Contents

IMPORTANT NOTICE - ACCEPTANCE OF THIS DOCUMENT

This policy and all associated policies applies to all full time and part time employees, casuals, volunteers, temporary/agency staff of the Council and all contracted third parties working for the Council and partner employees, whether they are working on school premises, at their offices or at any other premises, including their home.

As a minimum all new starters must read this full version of the CISP. Other staff may be made aware of their information security responsibilities by reading the summary version of the CISP dependent on their role and the nature of information they are accessing.

Where relevant you are **required** to have read the information in this document. **Please indicate that you have done so when you log on to your computer or by completing and signing the Acceptance Form at the end of this policy**

1. Introduction

1.1   Information can exist in many forms. It can be printed, written, stored electronically, transmitted by post, email, fax or even spoken in conversations. The purpose of information security is to ensure that all information (including personal information) and associated processing systems are protected to an adequate level to prevent distress or have any negative impact on the school and its services.

2. Scope

2.1   This policy sets out minimum standards and common acceptable use for confidentiality, integrity and availability of information to meet internal and legal requirements.

1	**Confidentiality**	Ensuring that information is accessible only to those authorised to have access
2	**Integrity**	Safeguarding accuracy and completeness of information and processing methods
3	**Availability**	Ensuring that authorised officers have access to information when required.

2.2   The policy has been written to conform, where possible, to standards such as ISO 27001 (Information Security Management standard), HMG Data Handling Guidelines and PCI-DSS (Payment Card Industry – Data Security Standard).

2.3   This policy supports all of the school's co-operative values but in particular contributes to the openness and honesty of School business by balancing the use of information with the implementation of measures to safeguard and respect this information.
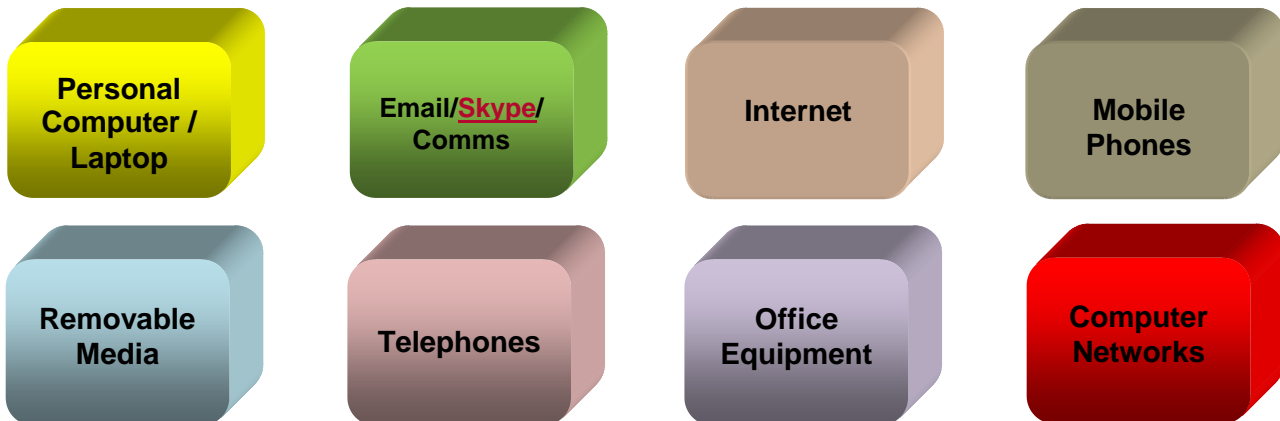
3. Roles & Responsibilities

3.1   All staff within the School have a responsibility to ensure that they take steps to safeguard the security of the information that they are using and seeing.

All staff must:

✔   Read and comply with this policy (including linked acceptable use policies)

✔   Read and comply with the Information Security Breach Procedure (ISBP) Procedure

✔   Be personally responsible for information held by them

4. Acceptable & Unacceptable Use

4.1   The School will not tolerate the use of any of its equipment/information for any purpose which contravenes this policy and associated policies/documentation. Staff found not complying with these requirements may be subject to disciplinary action. This policy covers the following areas of use:

Personal Computer / Laptop	Email/Skype/ Comms	Internet	Mobile Phones
Removable Media	Telephones	Office Equipment	Computer Networks

Staff should also ensure they are familiar with the requirements of other related policies on records management, data protection and social media.

5. Asset & Information Classification

5.1   In order to make sure that the School's information/assets receive an appropriate level of protection, all information will be treated in accordance with the requirements of ISO 27001 (Information Security Standard).

Asset Accountability - All major assets (and associated licenses), whether physical or information/software, have identified "owners". The asset owner is accountable for the maintenance of the asset. The ICT Coordinator maintains an asset register of ICT related equipment and software.

Information Classification – The school has a classification structure of information that will be used to inform future records management programmes

Information Labelling and Handling - Information being stored in whatever form should conform to labelling and handling standard (i.e. naming conventions) detailed in the Records Management Policy.

6. Information Sharing

IMPORTANT – KEY MESSAGES

- You should only share personal identifiable information (PII - Data about an individual that could, potentially identify that person) where there is legal justification to do so.
- You should know the objective/reasons for sharing PII.
- You should investigate whether the objective can be met without sharing PII.
- You should only send the minimum PII definitely needed to meet the objective/reasons.
- You should, where possible, anonymise the information you send so it is not personally identifiable
- You should confirm the recipients contact details, e.g. postal address, email address, etc. before sharing information
- You should appropriately protect the PII you are sharing either by using a secure solution if it is electronic, sending post by special delivery/courier, etc.

6.1   The school will, where there is a defined justifiable purpose, sign up to information sharing agreements with partner organisations, where these agreements are within the boundaries of applicable legislation and regulation and do not compromise the School or the confidentiality of the personal and/or sensitive data that it holds.

6.2   The School will have put in place information sharing agreements where regular sharing of information from School systems/records takes place.

6.3   Information Governance has produced a standard data sharing agreement checklist and will advise and guide Schools in developing data sharing agreements that cover specific requirements, suitable to their needs.

6.4   In order to ensure that information sharing takes place in an appropriate manner, all data sharing agreements should be approved by the Headteacher and comply with Information Governance requirements and the Information Commissioners Code of Practice on Data Sharing.

6.5.1   Receiving and sending confidential/personal information

School staff have control over confidential/personal information they send to other parties. It is critical that appropriate security measures are in place before information is sent out. Staff have little control over how other organisations or the public may send confidential or personal information to the Council. Staff must:

- post – send information via special delivery, or if sensitive or a large number of personal details are included, use a reliable courier who will deliver to a named recipient only. Consider hand delivery if local, to someone known to you. Senders should be encouraged to send confidential/personal information to the Council by special delivery/courier.

- email – only use secure email accounts such as GCSX and the Secure Communications System (SCS) to send personal information. Also recommend to senders that they use encryption/password protection for documents and where possible use secure email accounts such as GCSX or the Secure Communication System (SCS).

- fax – only to be used in exceptional circumstances. Should send to a known fax number only and verify the number before sending. Ask if the fax is a safe haven (area that is secure and

accessible only by authorised staff). If not request that the recipient stands and collects the fax as it is received. Also discourage senders from using faxes.

7. Physical and Environmental Security

7.1   All Staff have a responsibility for the physical security of School's assets (including information) including securing their laptops, locking away sensitive information, etc.

7.2   ICT will be responsible for the provision of suitable physical, technical, procedural and environmental security controls in line with best practice such as ITIL (Information Technology Infrastructure Library – standard for IT service management) in order to prevent unauthorised access to, interference with, or damage to information.

7.3 Access Control

7.3.1   The Senior Leadership Team have responsibility for authorising their own staff to access information including IT networks, offices, secure filing cabinets etc. No Staff employee may access or attempt to access any information for which they have not been given authorisation.

7.3.2   The Headteacher will remove access to information during periods of extended leave or sickness of more than 3 months. A review of employee's level of access to School information must be undertaken by their line manager during the 121 process.

7.3.3   Additional security measures shall be implemented by data owners to control access to especially personal/sensitive School data.

7.3.4   To control access to information, care must be taken (within the constraints of new ways of working) as to the physical positioning of desks and equipment used to view key personal, sensitive or confidential data. Desks used to process or view such data must be positioned away from doors/windows and public areas.

7.3.5   The Senior Leadership Team must ensure appropriate access controls are in place for information processed in open plan offices. Adequate clear desk arrangements should be adhered to as outlined in this policy.

7.4 Physical security (equipment)

7.4.1   Desktop machines in public areas must be secured to protect against theft or unauthorised access.

7.4.2   Multi-Functional Device (MFD) machines must be sited appropriately in areas where sensitive information can be handled.

7.4.3   Backup equipment and media must be sited at a safe distance to avoid damage from a disaster at the main site and must be subject to the same environmental and physical protection as the main system.

7.5 Security of premises

7.5.1   Access to areas containing sensitive School information must be strictly controlled and given on a need to know basis. A record of privileged access granted to nominated individuals will be kept by the respective Manager where necessary.

7.5.2   Physical security (door locks, locked cabinets, security card access) is the responsibility of all employees. Doors and windows must be locked as and when appropriate and blinds or curtains in place, with external protection considered for windows, particularly at ground and lower ground level.

7.5.3   All staff are issued with identity badges which include a photograph and these must be worn visibly at all times when working in School buildings. Staff must question anyone in the school building not wearing identification, where they are confident to do so. If staff are not confident in approaching someone, they must inform the SLT or their line manager immediately. Staff must understand that they may be asked for identification at any time.

7.5.4   Access to School premises is controlled by coded gates/key entry doors & electric gates. A combination of which are required to access the school building. Upon staff members leaving, keys are returned to the school office and codes are changed.

7.5.5   Passes for visitors are controlled by Reception. Visitors to School must not be allowed to wander around the buildings and must be accompanied at all times. They must sign in and out at Reception and wear identification badges visibly at all times.

8. Loss or Theft of Equipment/Files & Information

8.1   In the event of any loss/theft of equipment, files and information, the School's Information Security Breach Procedure should be followed. The key immediate actions include:

- Theft of equipment should be immediately reported to the police (obtain crime number) and to the Headteacher and ICT. The Head will then inform Insurance and IG.
- Theft/loss of files or information should be reported to the Headteacher and IG.

9. Staff/User Access Management

9.1   Staff registration

9.1.1   The Senior Leadership Team or data "owner" must authorise access to information / systems for the provisional user with access being granted on a 'need to use' basis in order to carry out their duties. Access should not be granted prior to authorisation being given.

9.2   Password responsibilities

9.2.1   Good, secure passwords are essential and staff must be aware of what constitutes a suitable password. The School's Password Management Policy should be adhered to at all times

In summary:

Passwords must be:	Passwords must NOT
• Changed regularly or immediately if there is any doubt at all that a password may have been compromised • Kept confidential and never shared • Changes at the first opportunity from default assigned passwords	• Be easily guessable, and this includes dates of birth, family names, pet names, or other personal details • Be shared with anyone else • Be the same as your system user id • Re-used on an alternate basis

• At least 8 characters long and complex, i.e. not be a simple word, name easily associated with you and contain numbers, a mixture of upper and lower case characters and allowed symbols	**Passwords should NOT** • Where possible be written down • Where possible be duplicates of passwords used for other systems.

The use of generic accounts and passwords for staff must be referred to ICT. ICT will consult with Information Governance on the validity of the request.

Staff can allow the Senior Leadership Team to reset their password via ICT Self-service.

9.3 Leaving procedure

9.3.1 When staff leave the School, as part of the School's leaver's procedure their Line Manager is required to:

- Ensure that any information held in the leaver's homes drive (H drive) or One Drive, that is of importance to the School, is moved to a relevant network folder
- Request accounts to access School systems to be deleted/disabled
- Ensure email accounts/contacts and membership of email group accounts are removed and, if appropriate, emails will be auto-responded to providing alternative contact details

9.4 Non-electronic media

9.4.1 Paper media (including carbon copies, computer printouts) containing information that is classified as personally identifiable or sensitive must be shredded on site. Disposal should be in line with the School's Record Retention Schedule.

9.5 Disposal of equipment

9.5.1 ICT equipment for disposal must be reported to the ICT Service Desk to enable them to arrange secure disposal. ICT equipment no longer required must not be used by staff for personal use.

9.6 Third party access to systems

9.6.1 It is the responsibility of data owners or Senior Leadership Team in conjunction with ICT to authorise third party access to resources and systems. User accounts and passwords will have to be created and where necessary relevant policies will have to be signed by the School and the third party prior to allowing access.

9.6.2 It is the responsibility of the relevant Senior Leadership Team member to advise ICT as soon as the third party access is no longer required.

9.7 Internet and intranet web publishing

9.7.1 Some staff will be authorised to publish data on the Intranet and Internet. This privilege must not be shared with staff who are not authorised to publish information.

9.7.2 Senior Leaders are responsible for content which is published and must ensure that the information is correct, timely and relevant and is published in plain English.

9.7.3 Inappropriate, illegal or offensive material must not be published. This will be removed and may result in disciplinary action being taken against the offender.

10. Working from Home and Mobile Working Overview

10.1   There is a difference between "working from home" and "home working" and "mobile working".

Working from Home	Home Working	Mobile Working
Work undertaken for limited periods but officer remains office based.	Officer's normal place of work is their home and they do not visit the office daily.	Officer travels as part of their role and will require access to Council facilities (network) whilst travelling.

Staff authorised as mobile workers or who may work from home **must**:

- Adhere to the School's home working and remote working guidance documents.
- only use School equipment to do their work unless accessing cloud services
- ensure that all equipment and information is kept secure at all times, including ensuring that any equipment or information is not left "on show" in parked cars etc.,
- never connect their School equipment to any other network (unless it's a home network to access corporate cloud) or non-Council equipment including personally owned equipment
- never send any work information of any type to "non-work" email addresses
- never dispose of any used media off-site – it should be disposed of via ICT

10.2   Staff are responsible for ensuring that unauthorised persons are not able to view confidential information or use School equipment. This includes family members and staff from other organisations.

10.3   Use of any confidential information at home must be for work purposes only. If the use of confidential information at home can be avoided, then the information should not be taken home.

10.4   Staff must ensure that when storing equipment/information at home, it is kept as secure as possible and if available is stored in a locked container.

11. Security Responsibilities for Staff and Delivery Units

11.1   All managers must make it clear to their staff, where the job description is not explicit, the level of responsibility that they have for information that they handle. This includes compliance with key elements of this policy including:

11.1.1 **Password management –** see section 9.2 of this policy and Password Management Policy.

11.1.2 **Encryption and cryptographic controls -** Appropriate encryption to be used to communicate / transfer data outside of the authority.

11.1.3 **System implementation and software purchase -** all system implementation and software purchases must be undertaken via the ICT Service Desk. Any projects that include the possible use of new computer systems/applications must engage ICT prior to discussions with suppliers.

11.1.4 **Clear screen and clear desk -** Staff must ensure that they lock their PC screen when leaving their desk for a limited time, or log out when leaving for extended periods.

Desks and other spaces must be kept clear of any confidential information at all times when the information is not being used and you leave your desk for a short period and locked away out of sight after a longer period.

11.1.5 People Services employment checks - All appointments must comply with School recruitment policy and include verification of an employee's identity, qualifications, employment history and eligibility to work in the UK.

11.1.6 Confidentiality agreements - As part of all employee's terms and conditions of employment, there is a requirement to maintain confidentiality of information both during and after their employment. Casual staff (including contractors/ agency staff) and third parties (including volunteers) not covered by an employment contract are required to sign a confidentiality agreement prior to being given access to information processing facilities. All such staff will be informed about the need to, and method for, maintaining confidentiality regardless of what access their role gives them to information.

11.1.7 Terms and conditions of employment - Employees of the School are expected to be aware of and comply with the all the codes of practice included within the Employee Code of Conduct, which includes responsibility for information security. Employees should also be aware that responsibility for information security continues beyond the end of their employment with the School and extends to all places and all times, including outside work. Breach of confidentiality can lead to summary dismissal within the Council's disciplinary procedure.

11.1.8 Training – regular training will be provided by the school to support staff in adhering to the policy.

12. Monitoring System Access, Use and Auditing

12.1   All systems may be monitored to detect unauthorised activity or potential security breaches.

12.2   Logged events may be reported to Headteacher and action taken if breaches or suspected breaches occur.

12.3   Monitoring will be undertaken in accordance with legislation (Lawful Business Practices Regulations 2000 and Regulation of Investigatory Powers Act).

12.4   The School reserves the right to monitor, log, collect and analyse the content of all transmissions on networks/applications, including internet and email/Skype usage, at any time for system performance and fault diagnostic purposes as well as to detect unauthorised use of systems and to ensure that systems are being used in accordance with acceptable use policies.

13. Communications & Operations Management

13.1   Illegal copying

13.1.1 Subject to the School's duty under Freedom of Information legislation Staff may not copy materials (including newspapers) protected under copyright or patent law or make any materials available to others for copying. Staff are responsible for complying with copyright or patent law and applicable licences that may apply to software, files, graphics, documents, messages and other materials you wish to download or copy.

13.2   Communication of trade secrets

13.2.1 Unless expressly authorised to do so staff are prohibited from sending, transmitting or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to the School or any other organisation.

13.3 Housekeeping

13.3.1 Senior Leaders should be aware of equipment, information or software that is taken off site. In all cases those personnel taking School property off-site will be responsible for the security of such equipment/information at all times.

13.3.2 Individuals must be made aware that they may face disciplinary procedures that could lead to dismissal if found responsible for the theft of equipment, software or School information.

13.3.3 Staff handling personal/sensitive information must take extra measures, e.g. encryption, password protection, use of lockable storage, etc, to ensure information in their possession remains private and secure in order to comply with the Data Protection Act 98 (replaced by General Data Protection Regulations [GDPR] from 25/5/18).

13.3.4 The unnecessary processing of sensitive personal data in an identifiable form must be avoided. The Headteacher is responsible for drawing up procedures in the school.

13.3.5 Documents and records must be stored under secure conditions up until the point that they are either destroyed/shredded at work or passed to a third party to carry out physical destruction. This means that they must not be left unsecured in skips, bins, reception areas, corridors etc.

13.3.6 Sensitive or confidential information must not be recorded on voice mail systems.

13.3.7 All employees should be aware of the risk of breaching confidentiality associated with the photocopying (duplication) of sensitive documents. Authorisation from the document owner must be obtained where documents are classified as 'highly confidential' or above.

13.4 Storage

13.4.1 All personal data stored electronically must comply with the Data Protection Act 1998 (or GDPR from 25/5/18).

13.4.2 The information created/stored by the School must be retained for a minimum period that meets both legal and business requirements as set out in the Corporate Information Retention Schedule.

13.4.3 Data is to be protected against loss, unauthorised or accidental changes, and may only be destroyed in accordance with data retention and destruction policies.

13.4.4 Hard copy documents that require archive storage should be securely stored within school using the appropriate filing arrangements

13.5 Audit trails

13.5.1 To protect both staff and the School, all systems have clear audit trails. This is particularly important for staff with administration rights.

13.6 Complying with legislation

13.6.1 Everyone has an obligation, under legislation such as Freedom of Information and Data Protection Acts (and GDPR from 25/5/18), to deal with information in the stipulated way. Further guidance on this can be obtained from Information Governance.

13.6.2 It is the responsibility of School Managers to make sure that staff are aware of any specific legislation applicable to their role including data protection.

14. Outsourcing

14.1 Any outsourcing must be with reputable companies that operate in accordance with quality standards. Such an undertaking must include a suitable Service Level Agreement (SLA), which meets the School's requirements. Where the processing of personal data is outsourced, a data processing agreement should be in place.

14.2 Where outsourcing includes the use of cloud computing the provider must provide assurance that cloud arrangements comply with recognised cloud security standards.

14.3 Any agreements or contracts must make it clear to the outsource organisation what their obligations are in respect of the Data Protection Act 1998 (GDPR from 25/5/18), Freedom of Information Act 2000 and other relevant information related legislation.

14.4 Outsourcing that may take place where information crosses outside UK and European borders must take into consideration the requirements of principle 8 of the Data Protection Act 1998 (GDPR from 25/5/18) – the restriction of movement of personal data across boundaries outside the European Economic Area (EEA). This maybe particularly relevant to new technologies such as cloud computing.

15. Systems Development & Maintenance

15.1 Controls will be implemented to ensure that security requirements are considered when developing existing information systems and prior to introducing new ones.

15.2 Information governance (IG) requirements of systems

15.2.1 IG will be involved in the development of new information system functionality (including new systems and development to existing systems) and processes that include the processing of personal information to ensure that all governance requirements are included.

15.3 Data input

15.3.1 Line managers will have responsibility to ensure their staff are aware of processes and procedures relating to quality of data input in line with local data quality policies / requirements.

15.4 Data output validation

15.4.1 Staff must undertake data quality checks on data output to ensure it is accurate/ up to date and complies with any local policies on data quality.

15.5 Security/Privacy requirements within projects

15.5.1 Project Managers are required to undertake a risk assessment/Privacy Impact Assessment (Data Protection Impact Assessments from 25/5/18) to identify security/data protection requirements for new School systems that process personal information.

15.6 Test environments and test data

15.6.1 Any systems being tested, or developed and tested will be separated from live systems. Live data will not be used and on logging in, the user(s) will be informed that they are in a testing environment. Where development of systems occurs via a third party, there will an expectation that all testing will be completed to the relevant ISO standard.

16. Business Continuity

16.1   The School has a process for management of business continuity.

17. Legal, Regulatory and Contractual Compliance

17.1   To avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and any security requirement, compliance with this policy is mandatory. Failure to comply with policy requirements will be viewed as a breach of security. Any such event may be the subject of investigation and possible further action in accordance with the Disciplinary Procedure.

17.2   All parts of the School will be subject to review to ensure compliance with this Policy. Audit & Governance may commence an investigation when the conditions of use have or may have been broken. Dependent on the circumstances staff may not be informed of the investigation. Whilst the investigation is under way, the staff member or account concerned may have their access rights suspended or reduced. If this occurs, the staff member will be informed.

17.3   Intellectual property rights (IPR) (also refer to section 13.1.1 of this policy)

17.3.1 Intellectual property rights include, but may not be limited to copyright, design and patents and trademarks.

17.3.2 Staff will not load software, video and audio files onto School systems without authorisation from ICT and that authorisation will include checking that any IPR has not been broken by the use of the software.

17.3.3 Licences for systems will be adhered to; including making sure that any restrictions in the number of users for a particular piece of software are complied with.

17.3.4 Copies of software and systems will not be made by staff unless authorised to do so by the licence holder and ICT.

17.4   Management of records

17.4.1 Information such as financial records, employee records, customer records and any records that are publicly accountable will be kept in accordance with ISO15489 records management recommended retention periods detailed in the School's Record Retention Policy

17.5   Data protection and personal information

17.5.1 All personal information managed by the School is covered by the Data Protection Act 1998 (GDPR from 25/5/18). This provides legislation as to how personal information may be used, stored, processed and shared. It contains eight principles (GDPR contains 6 principles) that the School should conform to and also governs how information needs to be handled under certain circumstances.

17.6   Freedom of Information (FOI)

17.6.1 The FOI Act 2000 governs access to non-personal information in public organisations. Any request for information to any member of staff, in written form, is a request under this legislation. Staff must respond to these requests if they can answer the question quickly (site opening times etc.) – known as business as usual requests. If it is a more in depth enquiry, or a decision is made to withhold information then the request should be passed to the Headteacher.

17.7 Environmental Information Regulations

17.7.1 The Environmental Information Regulations (2004) covers the provision of information that is environmental in nature.

Appendix A - Acceptance form

Corporate Information Security Policy – Acceptance Form

Local Authority	
School	
Full name	
Job title	
Contact telephone/email	

- I have read, understood, and agree to abide by Crudgington Primary School's Information Security Policy.

- I understand that this policy may change and that I will read any new versions when I am informed that they are available.

- I further understand that I must read, understand and agree to abide by the acceptable use policies and codes of practice that are relevant to me and that if I have any questions that I may ask the Headteacher for further information

Signed _____   **Date** _____