Sandwell
Community School

Information Security Policy

Contents

Information Security Checklist

Introduction

The purpose of this checklist and accompanying guidance is to support Sandwell Community School in ensuring the safety and security of any material of a personal or sensitive nature, or data that is important to the secure running of the school. Following this checklist and guidance will enable our school to comply with and follow government procedures in a way that is proportionate and appropriate. It addresses the key messages in:

- *The Data Protection http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_*
- *Data Handling Procedures in Government http://www.cabinetoffice.gov.uk/reports/data_handling.aspx*
- HMG Security Policy Framework.

  http://www.cabinetoffice.gov.uk/spf.aspx

The checklist highlights and defines the main areas for the school to consider and address. It also refers to a range of appendices which contain further detail to support this process. They represent the kind of technologies, products and procedures that schools should adopt. As new technologies are developed, schools will need to develop new systems and procedures to maintain and improve data security.

To protect data, schools may need to make operational and technological changes. Some can be accomplished quickly with existing resources whilst others may require extra investment and the help of ICT and suppliers. Schools will need to make staff more aware of data security through training. They will also need to put in place systems and procedures for:

- protectively marking data and impact levels
- encryption
- audit logging
- responding to security incidents
- secure remote access
- reviewing user access requirements for remote access to, and storage of, secured data

Information Security Checklist

Area	Definition	Question	Yes/ No	Appendix	Action (for school completion)
1 **Roles and Responsibilities**	This deals with the definition of roles and responsibilities.	Have key roles and responsibilities been identified? E.g. the Senior Information Risk Owner (SIRO) and Information Asset Owners (IAO)?		Appendix 1	
2 **Training and Awareness**	This deals with creating a culture or ethos in which the importance of information security is known and understood.	**Do all staff:** 1. receive training? 2. understand the importance of information security and data protection? 3. understand when email is secure and not secure? 4. understand sanctions		Appendix 2	All staff sign e-Safety Policy and receive annual training. New staff receive training as part of their Induction meeting with e-Safety Lead. All staff agree acceptance of terms at every log-in to the schools network.
3 **Data Protection**	This section includes a brief summary of the key elements of the Data Protection Act and includes Protective Markings.	Has the school identified and protectively marked data assets that contain personal data and sensitive personal data?		Appendix 3	
4 **Technical Controls: Access, privileges and permissions**	This deals with access and the privileges granted to users so that they may perform certain functions.	Does the school have set procedures for adding or removing users and assigning privileges from and onto: 1. The school network? 2. The MIS system? 3. The Learning Platform? 4. Other systems? 5. Restricted areas?		Appendix 4a	
Technical Controls: Identification	This deals with user names and how users identify themselves to the school network, other systems and areas.	Are well defined naming conventions established and maintained?		Appendix 4b	

Technical Controls: Secure Remote Access	Schools must secure any personal data that is removed or accessed from outside a secure area in the school.	Is the school using secure remote access technology, where appropriate, to secure the personal data of learners, staff and any other authorised users?		Appendix 4c	

5 **Passwords and authentication**	Authentication is how users prove to the systems they are who they claim to be.	Does the school have an appropriate policy in place?		Appendix 5	
6 **Hardware and Media (e.g. USB drive, CD, DVD)** **Security**	This deals with the physical security of important items such as servers and media. It deals with security in relation to data stored on media. It deals with the disposal of hardware and media.	Are the physical and data assets "protected" both inside and outside of school? Does the school have appropriate procedures in place for the disposal of hardware and media?		Appendix 6	
7 **Risk Assessment and Audit**	This deals with on-going checks of the security of all the school physical ICT and data assets.	Does the school have an on-going audit, monitoring and review process of all their physical ICT and data assets?		Appendix 7	
8 **Guidelines for dealing with an ICT** **Security Incident**	This deals with how to handle an ICT Security Incident.	Does the school have an ICT Security Incident Procedure in place?		Appendix 8	

9 **Other considerations**		Does the school consider data security: when providing online information for parents, developing and maintaining its website or VLE? CCTV - Does the school advise users to the site of its use?		Appendix 9	

Appendix 1: Roles and Responsibilities

School Responsibilities: It is the school's responsibility to ensure the security of their ICT assets and data. **All** members of the school community have a role to play in information security. It is the responsibility of each member of staff to adhere to the policy, standards and procedures.

The Role of the Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff within the school who is familiar with information risks and the school's response. Typically, the SIRO should be the head teacher and have the following responsibilities:

- 'own' the Information Security Policy
- establish standards, procedures and provide advice on their implementation •
- act as an advocate for information risk management

(The Office of Public Sector Information (OPSI) has produced a guide to Managing Information Risk, to support SIROs in their role. This is available online

http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf

Role of the Information Asset Owner (IAO)

Schools should then identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate. For example, the school's management information system should be identified as an asset and should have an IAO.

The role of an IAO is to understand:

- what information is held, and for what purposes
- how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result, the IAO is able to manage and address risks to the information and make sure that information handling complies with legal requirements. Typically, there may be several IAOs within an institution.

Any remote access to secured data must be authorised by the Information Asset Owner of that data.

Appendix 2: Training and Awareness Checklist

Description	Training Needs	Which Staff	Date Completed
Roles and Responsibilities	Appropriate SIRO and IAO training including dealing with ICT Security Incidents. Training has been given to all staff appropriate for their role.		
Acceptable Use Policies (AUP)	All Staff need to understand the terms and significance of acceptable use and internet security policies, including possible sanctions for breaches of such policies.		
User account management and access controls	Systems Training for authorised school staff which enables them to add, disable and delete user accounts. Training for authorised staff that are required to access restricted areas or documents within school.		
Password Management	All users to be made aware of the password guidelines appropriate to their role.		
Audit	No training required – Audit logs are created by Securus software which automatically tracks every action undertaken by users on the network.		
Hardware Security (including USB drives and other media e.g. CD's)	All users must receive guidance on the importance of safeguarding hardware and media. All users must receive appropriate training in the disposal of hardware and/or media.		
Use of Secure Remote Access	Training in the use of our learning platform (Google drive and Moodle/VLE).		

Appendix 3: Personal or Sensitive Personal Data

Context - Data Protection Act 1998

The Data Protection Act 1998 came into force on 1 March 2000, bringing the UK in line with a European Directive on Personal Data (95/46/EC)
http://www.dataprotection.ie/viewdoc.asp?DocID=92
The Act is there to protect the rights and freedoms of individuals, especially their right to privacy with respect to the processing of personal data. The Data Protection Act 1998 requires all schools to hold personal data securely.

Definition - Personal Data and Sensitive Personal Data

The Data Protection Act applies to *personal data* (data that applies to a living person) held on a computer system or on paper. **Personal data** is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This includes names, contact details, gender, dates of birth, academic achievements, other skills and abilities, progress in school and so on. Stricter rules apply to **sensitive personal data** including (but not limited to) special educational needs, health (mental or physical), religious beliefs, racial or ethnic origin and criminal offences. In an educational setting, 'sensitive' personal data would include, for example, data recording that a pupil was considered 'at risk', or that a member of staff had extended leave for mental health problems.

It is a legal requirement to protect personal data. Individuals entrusted with personal data, however derived, are accountable for its protection and compliance with the law.

The first step for all schools must therefore be to identify, within all the data they hold, which data counts as 'personal' and 'sensitive personal'.

Fair Processing

Personal data must be processed in accordance with certain principles and conditions. Anyone who processes personal information must make sure that personal information is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- processed in line with the individual's rights
- secure

Personal data can only be processed under one or more of the following rules:

- an individual has given consent
- it is part of a contract

- it is a legal obligation
- it is necessary to protect the individual
- it is necessary to carry out public functions
- it is in the legitimate interests of the data controller

While explicit consent must be obtained in many contexts, consent is not required for the purposes of delivering an education within the education sector. However, the reasons for collecting and processing sensitive personal data must be completely transparent.

Other data

Although not defined as personal data, schools should also secure any data that is *critical* to the running of their school. This might include, for example, all financial data as well as a wide range of correspondence. Schools need to consider the risk of financial loss not only to them but also to another party if there was a breach of security.

Protective Marking and Impact Levels

Once data has been identified, protective marking should be applied. Protective marking is the method by which the ***originator*** of information indicates to others the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside the originator's own school, department or section and its ultimate method of disposal.

A key element in determining protective marking is the impact it would have on an individual or individuals if it was lost. This is known as the impact level. It is good practice to apply protective marking to all documents, based on the impact level.

There are seven impact levels already defined ranging from 0 to 6 however, most schools are only likely to use the following four:

- Impact Level 0 (IL0 and 1) Not protectively marked / Unclassified
- Impact Level 2 (IL2) Protect
- Impact Level 3 (IL3) Restrict

There are full definitions of impact levels at

http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/media/204715/business_impact_level_tables.pdf

The summaries below will help determine the appropriate impact level.

Impact Level 0 and 1 (IL0 and 1) Not protectively marked / Unclassified:

Most school documentation from which no living individual can be identified falls into this category. Examples are School prospectus, policies, general letters about school activities, invites to parent evenings etc.

Impact Level 2 (IL2) Protect:

A school document that contains personal but not sensitive information which (enables a living individual to be identified and) if lost or sent to the wrong destination may cause inconvenience, embarrassment, loss of reputation, harm or distress to an individual or school should be marked **Protect.** Examples are requests to correct or amend information supplied by the local authority for less than 10 pupils / staff, personal letters to parents detailing with an incident involving their child e.g. behaviour, attendance or achievement.

Impact Level 3 (IL3) Restrict:

Sensitive personal data is information that relates to race and, ethnicity, political opinions, religious beliefs, membership of trade, unions, physical or mental health, sexuality and criminal offences. A school document which contains sensitive personal information relating to any individual should be marked **Restrict.** Examples are statutory data returns (school census, workforce census, assessment), education plans (IEP's, PEP's,), Child Protection referrals.

Personal data on a significant number of individuals i.e. 10 or more, should also be marked **Restrict**.

Examples of protective marking in practice

Learner details exported from the MIS

A typical export of learners' details from the management information system (MIS) might include sensitive personal data such as medical data and notes and ethnic origin. Schools should mark any electronic or printed exports of this data with the appropriate protective marking (likely to be either PROTECT or, in some cases, RESTRICT). Schools may also add extra notes (see above), instructing handlers to securely delete or destroy the data after use.

Emergency contact information for a field trip

Staff need to take emergency contact/medical data with them when taking learners on a field trip. The data may be held on paper, electronically, or both. Schools should ensure that staff keep the data as secure as is practical. However, they should balance this against the need to make sure that the data is readily available to staff when they need it. Staff should make sure that they securely destroy the data when it is no longer needed.

Destruction / Disposal markings

When personal data is no longer relevant to the purpose for which it was originally obtained, and/or has reached the end of the period for which it must legally be retained, it must be securely destroyed in accordance with its relevant protective marking.

When disposing of records or information which may contain personal data, schools must consider the nature of the information and the harm that may result through unauthorised use. The method of destruction should take into account the type of information. In all cases it must be ensured that disposing of data creates little risk of an unauthorised third party using it to the data subject's detriment. Where data is of a confidential nature (e.g. Protective marking of Protect and higher) and is held on paper records, then it should be cross-shredded or pulped.

For records held electronically these should be scrubbed clean or destroyed in accordance with industry best practice. Schools may include extra handling instructions to help staff remember to securely delete or destroy data. These could be part of the labelling scheme schools use, such as including destruction markings in the footer of a document.

Storage and access control

Access to any data or documents marked **PROTECT** or higher will need to be controlled by the school. Where documents are in printed form, they should be secured in a locked cabinet or area, and access restricted to appropriate personnel only. Access to electronic data or documents needs to be controlled by effective access rights set by the system, and backed up by 'strong' passwords.

Data that is marked **PROTECT** or higher should be stored in separate system folders or directories, and not share folders with documents with lower markings. This will help to restrict access to authorised people.

Transfer of Data / Information

Personal data must be sent by secure means and not by using open emails.
Frequently, schools need to move documents between systems e.g. when making returns to the local authority or awarding bodies, or when learners transfer between schools. Schools should make sure that they maintain protective markings and that the overall level of risk of a security breach does not increase because of the move. All data that is marked '**Protect**' or higher should be **encrypted before** transfer.

Transfer Methods Available

Schools have a range of ways in which information can be transferred. The method used is determined by the impact level identified.

Marking	Method
Impact Level 0 and 1 (IL0 and 1) **Not protectively marked / Unclassified**	Unsecured email. Any Post including internal LA courier service. Any Fax.
Impact Level 2 (IL2) **Protect**	Secured email encrypted in transit but personal data should be encrypted first (e.g. OPENHIVE mail between schools and third parties). If using non electronic mail, consider special delivery from Royal Mail or similar service.
Impact Level 3 (IL3) **Restrict**	Secured email encrypted in transit but personal sensitive data should be encrypted first (e.g. OPENHIVE mail between schools and LA). Special Delivery post from Royal Mail or similar. Double enveloped.

Other systems exist for specific information exchanges between schools and/or DfE, these include:
Web Exchange: Only to be used for Common Transfer Form (CTF) files to be sent from and to any maintained school.

Requests for Personal or Sensitive Personal data.

When a request is made, whether in person, on the telephone or by any other means, before releasing any information always authenticate the individuals identity and right to have the information. Often you will know who the person is but if in doubt do not release the

information until further assurance/proof is provided. You could ask a telephone caller to give you their phone number and call them back later, ask the personal visitor to provide proof of identity/responsibility, ask an official representing another body e.g.
Police or LA, to provide you with their line manager’s number and check with them.

The table overleaf gives a brief summary of information disclosure guidelines.

DISCLOSURE METHOD	**(IL0 and 1)** **UNCLASSIFIED**	**(IL2)** **PROTECT**	**(IL3)** **RESTRICTED**
Internal Post	Normal use	• Sealed envelope fully addressed to named individual or job title. • Mark envelope: **PROTECT.** • Consider tamper-proof envelopes. Electronic media must be encrypted.	• Sealed envelope fully addressed to named individual or job title. • Mark envelope: **RESTRICTED.** • Consider tamper-proof envelopes. Electronic media must be encrypted.
External Post	Ordinary envelope through public mail system	• Single envelope. Fully addressed including postcode, to named individual or job title. • Include return address. **Do not mark envelope with protective marking or descriptor.** • Consider tamper-proof envelopes. Electronic media. • Do not use USB pen drives even if encrypted.	• Single envelope. Fully addressed including postcode, to named individual or job title. • Include return address. • **Do not mark envelope with protective marking or descriptor, may use 'Addressee Only'.** • Consider tamper-proof envelopes. Electronic media. • Do not use USB pen drives even if encrypted. • Consider Special Delivery, Courier or personal delivery/collection.
Faxing	Allowed for normal use	Not allowed.	Not allowed.
Telephone and other Verbal conversations	Normal use	• Telephones can be used. • Confirm caller identity. • Do not disclose, either on telephone or in person, in public places (e.g. motorway service stations, shops, reception areas) where you could be overheard by people not entitled to information. • **Do not leave Protect information on voicemail**	• Telephones can be used • Confirm caller identity • Do not disclose, either on telephone or in person, in public places (e.g. motorway service stations, shops, reception areas) where you could be overheard by people not entitled to information • **Do not leave Restricted information on voicemail**
Email	Allowed	• Secured email encrypted in transit but personal data should be encrypted first (e.g. OPENHIVEmail between schools and third parties). • In subject field before any other information or title: [IL2: PROTECT].	• Secured email encrypted in transit but sensitive personal data should be encrypted first (e.g. OPENHIVEmail between schools and LA). • In subject field before any other information or title: [IL3: RESTRICTED].

Messaging Services	Allowed: Short Messaging Service (SMS) / Multi-Media Messaging Service (MMS) / Instant Messaging (IM).	Do not use Short Messaging Service (SMS) MultiMedia Messaging Service (MMS) Instant Messaging (IM).	Do not use Short Messaging Service (SMS) / MultiMedia Messaging Service (MMS) / Instant Messaging (IM).

Appendix 4 Technical Controls

a: Access, privileges and permissions

The school is responsible for the maintenance of its user accounts. The school will need to have a robust process in place for the addition and removal of accounts. It must also identify the access rights and privileges of all users to ensure they only have access to what is appropriate to their role.

Maintenance of accounts

As new staff and students arrive, user IDs will need to be set up. A leaver's administration process must ensure all permissions to systems are revoked at the earliest opportunity after the person has left the school. Best practise suggests disabling their network accounts and access to other systems e.g. email accounts, access to the MIS application, Learning Platform etc. as soon as they have left to prevent remote access by them or other individuals.

Agilisys and an authorised staff member will be responsible for maintaining the integrity of user access rights within the school network, the MIS application and the Learning Platform application based on the roles the users are assigned to.

Where automated provisioning is enabled pupils and staff added to the MIS application will automatically be provisioned with, the Learning Platform, Alfie Assessment, Doddle T&L Resources. When staff and pupils are removed from the MIS application their accounts are disabled and removed from the school's systems.

Where automated provisioning is not enabled, then the user accounts will have to be maintained separately from other school systems. The authorised staff member in the school can add and delete accounts and change passwords for users.

Learning Platform (OPENHIVEmail, Google Drive and VLE/Moodle).

Pupils and staff added to the MIS application will be automatically provisioned within the Learning Platform by Agilisys and an authorised member of staff. When staff or pupils are removed from the MIS application their portal accounts are disabled and removed from the school's portal.

b: Identification

Identification is the mechanism by which the system asks the user, "Who are you?" Users identify themselves to the system by means of a user ID (also referred to as a user name or log on name). A well-defined naming convention has the following characteristics:

- A logon-naming standard that clearly addresses all name characteristics.
- User IDs which are easy for users to remember.
- User IDs which are easy for administrators to create.

For access to some systems multiple levels of identification may be required.

c: Secure Remote Access

Schools must secure any personal data that is removed or accessed from outside a secure area in the school.

They must also ensure that sensitive and personal data is encrypted when it is in transit from one location to another, including transit from one approved secure area to another.

Providing secure remote access to systems and the personal data they contain requires multiple technologies that cover:

- **authentication** – who or what system is trying to connect, ensuring that the users and the computers at each end are who they say they are.
- **authorisation** – ensuring that the users at the remote end are authorised to access the data.
- **encryption** – to secure personal data in transit, and file or full disk encryption for any storage media that holds personal data.
- **audit** – logs of access to secured data.

Risk Assessment and Remote Access Requirements

Schools should think carefully about what kinds of sensitive and personal data they are making available remotely and who they are granting access to. Remote access to any personal data should be over an encrypted connection protected by a username/ID and password. Schools may receive data from other schools for example, on looked-after children or exclusions that may have been marked as having specific security requirements. Schools should include any protective markings on such data in their risk assessments. Schools should ensure that users are aware of the need to keep their sign-on credentials secure. This is particularly important when users access systems from a shared computer. For example, users should make sure they sign off when they have ended their session. Users should not save passwords, if offered this option by their browser. Users should ensure that unauthorised users are not able to use their credentials to gain authorised access, for example, another family member at home who may use a shared computer. Staff should not download personal data to their PCs, mobile phone or laptop.

Encrypting data in transit

Data in transit is any type of data that is transmitted between systems, applications or locations. Schools must encrypt personal data in transit.

Appendix 5: Passwords and Authentication

A password is the mechanism by which the system asks the user, “Is that really you?” It is vital that users **do not share passwords**.

It is very important for a school to establish password guidelines and to ensure that every user in the school follows these.

For staff a good password provides a high level of security and has the following characteristics.

✓	It is at least eight characters long and it is alphanumeric (consisting of both numbers and letters)
✓	It is a mixture of at least one lowercase and uppercase letter and at least one digit

For pupils, it is necessary to strike a balance between practicality and security.

For access to some systems multiple levels of authentication may be required.

Appendix 6: Hardware and Media

All users should receive guidance on the importance of safeguarding hardware and media

Media is any item that can hold data, this includes floppy disks, CDs, printed output, tapes, memory sticks etc.

Hardware and Media Guidance

Workstations with access to sensitive material **must** be password protected when left unattended.
Sensitive material **must** not be left unattended or unsecured at any time.
Sensitive information sent to printers **must** be removed from the printer immediately.
Users **must** protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software and appropriate logon mechanisms.
When sensitive or personal data is required by an authorised user from outside the school's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the learning platform (Google Drive or VLE/Moodle).
If secure remote access is not possible, users **must** only remove or copy personal or sensitive data from the school or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location.
School or users **must** securely delete sensitive or personal data when it is no longer required.
Servers must be kept in a locked room and access to that room must be controlled.

Secure Disposal of Hardware and Media.

When a school disposes of hardware which it owns it must ensure that any protected data is securely deleted preferably using appropriate LA preferred suppliers. The school must obtain documentation confirming that hardware has been disposed of appropriately and data securely deleted.
Hardware acquired under Lease / Hire arrangements will need to be returned to the appropriate lease hire company. The school must obtain documentation confirming that hardware has been disposed of appropriately and data securely deleted. This includes digital photocopiers that store copies of all printed documents on the internal hard drive.
A record of the disposal of assets must be maintained for audit purposes.
The school must dispose of hardcopies of any data marked protect or higher when no longer required by cross shredding, pulping or incineration. Or use if available DCS confidential waste sacks.

Appendix 7: Risk Assessment and Audit

Conducting an Information Risk Assessment

Schools should work out criteria for assessing risks. Criteria will need to take into account:

- the assets involved (physical and information)
- legal requirements (such as the Data Protection Act 1998)
- the practicalities of running the school day to day • the impact of incidents on reputation in the community.

Schools should then identify, describe and prioritise risks against these criteria. The first step in identifying risks is for Information Asset Owners to list both physical assets and information assets that contain personal data or data valuable to the school.

Steps in identifying risks include:

- assets • threats
- existing controls • vulnerabilities
- consequences

Once schools have identified risks they can estimate the size of those risks, that is, the combination of consequence and likelihood.

ICT Hardware Asset Register (Physical Assets)

Schools need to maintain an ICT hardware asset register which lists **all**. Regular hardware audits should be carried out, at least once a year, to ensure the assets are present and working.

Schools need to ensure **all** hardware; especially the servers are kept physically secure. Software and data related events are audited by Agilisys.

Agilisys and Broadband Sandwell maintains audit logs for all infrastructure equipment including servers, routers, firewalls, email, portal, SIMS and can provide logs on request to assist in an investigation.

Schools can also obtain web access logs and can view incidents of inappropriate use with Securus. Note that it is not possible to audit all the activities carried out on unmanaged computers in schools but it is possible to show that an unmanaged computer accessed some system resources.

Appendix 8: Guidelines for dealing with an ICT Security Incident

An incident can be defined as any real or suspected event in relation to the security of data or ICT systems. This can include anything from a lost password to the successful access to confidential data by a hacker.

Upon the discovery of a serious ICT security incident, the SIRO needs to evaluate and assess the situation and respond as indicated in the table below

Severity	SIRO/school evaluation	School Action/Response
Minor	The School can resolve the issue.	Dealt with in school and logged as part of the ongoing audit process. The school may wish to contact Governors to confirm its action.
Significant	The School is uncertain as to whether it may resolve the issue.	Contact Data Security and Compliance Officer (James Trickett) for advice.
Critical	The School cannot resolve the issue.	Contact Data Security and Compliance Officer (James Trickett) for advice.

For a **critical** incident the following procedure will be invoked:

- A management commitment and priority will be given to resolving the incident.
- A resolution team will be established.
- A primary responsible person for each incident will be established.
- A communications plan, including escalation procedures plan of action for rapid resolution will be established.
- The steps undertaken will be logged.
- A plan of action for non-recurrence will be established.
- A knowledge base of past security incidents, including steps taken for resolution and non-recurrence will be utilised.
- An awareness campaign where appropriate will be undertaken.

Appendix 9: Other considerations

Data security and online information for parents/carers

Schools using a range of technologies such as websites, learning platforms, email and text messages in order to encourage parental engagement with children's learning will also need to consider data security. The table below shows some of the ways that schools can exploit ICT while at the same time ensuring data security.

	Typical information	Technology available	Notes on Protective Markings
School life and events	School term times, holidays, training days, the curriculum, sports events and results, extra-curricular activities, events, displays of pupils' work, lunchtime menus, extended services, parent consultation, homework resources, school prospectus.	Common practice is to use publicly accessible technology such as school websites or VLE, and downloadable or emailed newsletters. Services such as email and text messaging can also provide updated information where parents opt for this.	Most of this information will fall into the NOT PROTECTIVELY MARKED category.
Learning and achievement	Information on how parents can support their individual child's learning, individual learners' academic achievements, assessments, attainment, progress with learning, learning behaviour, personalised curriculum and Individual Education Plans for learners with special educational needs.	Schools will make information available by parents logging on to systems that provide them with appropriately secure access. Examples include: a secure area of the school's network or a learning platform. Schools could also send communications to a personal device or email account belonging to the parent/carer.	Most of this information will fall into the PROTECT category. There may be learners whose personal data requires a RESTRICT marking or higher (for example, the home address of a child at risk). In this case, the school may decide not to make this learner's record available in this way.
Messages and alerts	Alerts and messages regarding information held by the school, such as individual learners' attendance, behaviour and special educational needs.	Email and text messaging are increasingly used by schools to contact and inform parents. Messaging systems integrated with management information systems and learning platforms are able to manage what information is available online or sent to parents using email and text messages. Learning platforms might be used to provide secure access to further detail and context.	Most of this information will fall into the PROTECT category. Although it may be possible to encrypt email or text messages to parents, schools should not send detailed sensitive information in this way. A telephone call or face to-face meeting may be more appropriate.

Special Security Considerations for Online Reporting

If a school intends to provide on line parental access to information about their children it should work out the remote access requirements by conducting a risk assessment on the data to be reported and ensure the content of the data provided is suitable for the parent to view. Schools should also look carefully at the content of the data they are making available to parents, to ensure that it does not reveal the personal data of other learners. It is also good practice to issue each parent with individual usernames/IDs and passwords so that access can be tightly controlled.

Websites/VLE

A school website is a useful tool to help parents and pupils view information about the school. However schools must ensure no individual children can be identified or contacted either via the school website or as a result of a visitor using it. Websites should not include personal details or names of any child or adult in photographs, only group photos should be used, personal email/postal addresses or telephone/fax numbers should not be used. Parents' permission to include children's work/photographs/input to the site must be obtained. For every piece of information, example of pupils' work, picture or photograph, ask yourself: could this have another purpose in the eyes of a visitor?
For more advice on Internet safety, visit the Sandwell Safeguarding Board website http://www.sandwelllscb.org.uk/site/professionals.html

Personal information online

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/personal_information_online.aspx

Cloud Computing

http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

It must be remembered that the data protection act still applies to websites.

Photographs

Sandwell Safeguarding Children Board website:
http://www.sandwelllscb.org.uk/site/professionals.html

CCTV

Increasingly schools are using CCTV to monitor the security of premises. Capturing and/or recording identifiable individuals is processing personal information and so needs to be done in line with data protection principles.

All users of the site must be made aware of the use of CCTV and of the purpose of its use. Cameras should only be sited where they are needed, used for their intended purpose and where they will not unnecessarily intrude anyone's privacy. Thought should also be given to the retention and access to the recordings. Remember CCTV images can be requested by individuals through a subject access request.

Further information on CCTV code of practice is available from the Information Commissioners website:
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx

Information Security Management Support for SCS provided by Agilisys

Agilisys, as the managed service provider, will support Sandwell Community School with their management of Information Security by providing and supporting the following;

Access Controls

- A means of adding and removing users to the school network and assigning them appropriate access to information.
- Control of access to electronic data held on school network servers including secure remote access for staff if required.
- Secure access to the school MIS data in school.

Authentication

- A means of enforcing password policies.

Control and Audit

- A means of auditing managed service computer and application use in school.
- A configured user environment preventing unauthorised application usage and suitable secure access to network resources.
- Operating system and application maintenance of managed computers.
- Maintenance of anti-virus software on the managed service network.
- Firewall protection of the schools network from outside access.
- Secure access to the internet for unmanaged devices using guest wireless access.
- Advice on tools to encrypt data.
- The option to purchase validated encrypted removable storage devices.
- Appropriate network management practices where carried out by Agilisys staff.
- A means to access audit logs for website access in school.
- A means to monitor inappropriate use by capturing screenshots when certain words and phrases are used on-screen.
- Access to relevant sections of audit logs from infrastructure equipment to assist with incident investigations.

Data Integrity

Agilisys will ensure data residing on managed computers and servers is secured, virus protected and backed up to ensure integrity. Schools should ensure any data transferred to and from managed computers is similarly maintained. This will require schools to ensure all non-managed computers that access school data whether they are in school or elsewhere are secured, virus protected and backed up and that the integrity of the disks and removable media is maintained with regular checks using operating system built in system tools as a minimum.

For removable media like USB drives it is important to eject the disks properly before removing them

- A file and folder backup and restore process for managed servers.
- A server recovery process in the event of catastrophic hardware failure.

Hardware and Media Security

Agilisys will provide:

- Secure off-site data backups.
- Secure hardware handling during maintenance.
- Secure hard disk disposal including data erasure using government approved methods.
- Disposal of Agilisys managed equipment.

When a computer is replaced as part of a refresh programme the whole computer will be stored in a secure local facility before being collected by a designated disposal company who will erase the data on any hard disks using methods approved by the UK and US governments. Server disks will be wiped before they are removed from the school.

The computer will then be broken up and recycled or sent to a charity for reuse overseas where possible.

All disposal processes are carried out in accordance with the Waste Electrical and Electronic Equipment Directive (WEEE Directive).

Leavers – Checklist for Managers

Please complete this checklist as appropriate, ensuring it is signed, dated and returned to the office for audit purposes. Please note it is your responsibility to ensure that the items below are returned as detailed.

Employee Name	
Campus	
Post Title	

Please ensure return of:	**Tick**	**Initial**
ID Badge returned		
School Property (keys, fob etc.)		
School data (paper files, CDs, removable media etc.)		
School hardware (laptop, mobile device, mobile phone, memory stick etc.)		
IT considerations	**Tick**	**Initial**
SIMS database amended		
Email account(s) disabled		
Active Directory Account disabled		
Access to external websites disabled (VLE, Alfie, etc.)		

This declaration is to be signed by the employee and line manager to confirm that all school equipment and information has been returned or destroyed as appropriate. Please understand that the school will seek to recover any claims/damages made against them as a result of inappropriate use of information.

Employee signature	
Date	
Manager signature	
Date	

Ratification

Signed:………………………………………………. T Lecointe

Acting Executive Head Teacher:

Date:

Signed:………………………………………………. D Smith

Acting Executive Head Teacher:

Date:

Signed:…………………………………………………. J McBride

Chair of Governors:

Date:

Implementation: 27.09.16 (Academic Year 2016-17)

Review Date: September 2017