School Systems and Data Security Policy

September 2016

POLICY NO.: 85
TEACHER: ANGELA MACVIE
LAST UPDATED: 03/10/16

CONTENTS

School Systems and Data Security Policy Details

Teacher Responsible: Mrs Angela Macvie

Ratified by Governing Body on:

Next review date: September 2019

1. **Introduction**

1.1. Chadsgrove School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions or statutory obligations. Chadsgrove also deals with large quantities of information that is not regarded as personal in terms of the Data Protection Act but nevertheless is important to the smooth running of the school.

1.2. All data is stored and managed using a network of computers and manual filing systems.

1.3. This policy deals specifically with how computer systems and the information stored within them are kept safe and secure. It also addresses how data that is not stored electronically is kept safe and secure.

1.4. The policy aims to ensure that:

- the confidentiality, integrity and availability of school information and assets are protected
- all users are aware of and fully comply with relevant legislation
- all staff understand the need for information and ICT security and their own responsibilities in this respect

1.5. Separate policies are available that deal, in greater detail, with the schools obligations with regard to the Data Protection Act 1988 and the Freedom of Information Act 2000 and these should be read in conjunction with this policy.

2. Physical Security

2.1. Physical security is about ensuring the protection of information by storing it securely and restricting access to it. Chadsgrove School aims to protect the school's investments in ICT from possible theft and to protect valuable or confidential data. The following physical security solutions are in place:

- The ICT suite is a room with no direct entry from the outside
- The server is in a locked cabinet
- All administration machines that hold personal data are in rooms that are locked when the school is closed
- The files of pupils who are currently on roll are stored in lockable cabinets in the Headteachers office
- The files of pupils who have left and any other confidential information that needs to be retained are stored in a secure room that is kept locked at all times
- Staff are requested to transfer files from mobile devices such as cameras and iPads to a computer as soon as possible in order to minimise the risk of loss and the risk of personal data falling into unauthorised hands.

3. Logical Security

3.1. Logical security is about ensuring the protection of information by protecting computer files using the following methods, all of which will be described in more detail later in the policy:

- Encryption – to prevent unauthorised access to data
- Network access restrictions - to ensure that users only see the information that they are authorised to
- Backup Procedures – to ensure that any lost data can be retrieved
- Passwords – to prevent unauthorised access to sensitive or confidential data

4. Procedural security

4.1. Procedural security is about ensuring that those staff who access personal data are authorised to access it, are appropriately trained and that personal data is disposed of safely and securely. The following procedural security measures are in place:

- Personal or sensitive data held on shared network spaces is only available through staff logons.
- Access to SIMS (personal information), SAP (financial information) and office-based data are restricted to specific machines and to identified individuals through user names and passwords.
- Administrative machines in the school office operate on their own 'mini' network that is not accessible from other machines in school unless a link has been specifically 'mapped' to it by the CIS technician and authorised by the Head Teacher or strategic ICT lead.
- The hard drives of computers that contain personal information are disposed of by a third party recycling company on the school's behalf and a certificate of data destruction obtained.

5. Encryption

5.1. Encryption is a process whereby the data held on a computer is encoded so that it can only be accessed by an authorised user. Once a hard drive has been encrypted, it is not possible to retrieve any data from the drive unless a legitimate user logs in. It is also impossible to access the data by connecting the hard drive to another computer without the correct credentials.

5.2. Any computers or laptops that may be removed (or stolen) from the school and that contain sensitive data are encrypted. Microsoft Bit Locker is used for this purpose. Servers are not encrypted, on the advice of the CIS technician, as adequate technical solutions are not yet available. Instead the server is protected by physical security as it is kept in a room which is locked when the school is closed.

5.3. School staff are advised not to use memory sticks to store personal or sensitive information. If this is unavoidable, for whatever reason, the use of external hard drives that are password protected is advised.

6. Curriculum Network

6.1. The setup of the school network provides the tools that are necessary for users to access the resources that it provides whilst restricting access to just the parts of the system that are appropriate. This is achieved through the use of user names and passwords (where appropriate) linked to specific logon scripts – depending upon the credentials entered, the server loads the appropriate resources for that particular individual.

6.2. In order to manage the network, Chadsgrove uses Windows Group Policy in conjunction with Windows Server 2012. Group policies are managed by the CIS technician and strategic ICT lead, who is also a member of the Senior Leadership Team. The strategic ICT lead is responsible for authorising any changes to group policy. Group Policy is used to effectively manage users and desktops as well as control access to printers, software and computers.

6.3. In addition, in order to create a manageable and secure school network, a range of management tools are available to the network administrator in order to simplify tasks such as:
- Managing users - resetting passwords quickly and easily, importing the details of new users.
- Managing printers
- Managing desktops - so that users see a suitable selection of program icons on the desktop
- Managing software so that packages can easily be installed and distributed around the system, without the technician having to visit every computer
- Managing computers so that the technician can rebuild corrupted machines quickly and easily, using a standard setup

6.4. All users must log on and staff are also required to provide a password as they are able to access sensitive data such as annual review information.

6.5. All users are required to use the school's proxy server in order to gain access to the internet. This ensures that the content filtering service is always functional.

6.6. Users are not able to install or uninstall software. This reduces the risk of a computer becoming corrupted or infected with viruses etc.

6.7. Users are not able to browse the network neighbourhood as they do not normally need to know which other machines are connected to the system.

6.8. All guest users are restricted to basic functionality using a visitor login. Visitor logins do not gain access to any sensitive/confidential information stored on the school network.

7. Back Up Procedures

7.1. In order to ensure that information can be retrieved in the event of a loss, the following back up procedures take place using scheduled systems:
- Chadsgrove Curriculum Server - daily automatic backups (not encrypted).
- Media Servers – saved onto the 'old' curriculum server with a weekly automatic back up to a QNAP NAS drive (not encrypted)
- SIMS / MIS Data (centrally hosted) – backed up at County Hall using Worcestershire County Council procedures and encrypted using 256bit encryption zip files. A copy is sent to IBS schools as part of the Disaster Recovery Plan
- SAP – backed up at County Hall using Worcestershire County Council procedures and encrypted using 256bit encryption zip files. A full Disaster Recovery Plan is in place.
- Sims share on office computer – backed up onto a memory stick with 250bit encryption using procedures supplied by Capita IBS Schools
- Office Data Drive and CASPA– backed up onto two memory sticks stored, one of which is in a locked cabinet and the other in a fire proof box
- Other office documents stored on the 'P' drive - backed up onto tape (not encrypted)
- Outreach Data – backed up onto two memory sticks, one of which is stored in a locked cabinet
- RM Maths – hosted and backed up by supplier
- BSquared – hosted and backed up by supplier

Backup procedures are described in more detail in Appendix 1.

7.2. No data is stored on the hard drives of any machines that are connected to the school network as these are not backed up. Teachers may store data that is not personal (as defined by the Data

Protection Act 1988) on the hard drive of their laptops. However, they then become responsible for backing up that data on to a suitable external device or media.

7.3. Monthly tests and reviews of backup procedures take place. This will be performed by the CIS technician in liaison with the strategic ICT lead.

8. Passwords

8.1. Passwords are integral to data security at Chadsgrove. Staff are made aware of the password policy (see Appendix 2) and are expected to implement it carefully. Critical passwords are stored in the school safe. According to the password policy, good or strong passwords:

- are 8 or more characters in length
- contain numbers as well as letters
- contain symbols or non alpha-numeric characters
- are easy to remember, but hard to guess
- are reasonable to type – staff should not have to resort to writing them down

8.2. Staff are requested not to:

- save passwords in web browsers if offered to do so
- use usernames as passwords
- use names as passwords
- email passwords or share them in an instant message.

8.3. In order to access systems such as Edulink, email or other systems linked to children's services, all staff and pupils need to use a Global ID and password.

8.4. In order to access the school network, adults are required to use an individual user name and password but pupils only need to use a class user name without a password.

8.5. In order to download confidential documents sent from the Local Authority via secure communications, authorised individuals are required to use two factor authentication (user name, password followed by an access code generated by the secure communications website and sent to the user's email or mobile phone).

9. School WI-FI Security

9.1. Chadsgrove School has a Wi-Fi network that is used to provide staff and pupil laptops with wireless access to the school network and the Internet. In order to guard against unauthorised use of this network, it is authenticated and encrypted using WPA2-PSK (TKIP/AES) technology, as recommended by Capita IBS Schools. The network was professionally installed and is maintained, when necessary, by County Infrastructure Services.

10. Email, Messaging and Secure Communication

10.1. Chadsgrove School uses county standard mailbox and domain names - office@chadsgrove.worcs.sch.uk and head@chadsgrove.worcs.sch.uk which conform to national standards. This ensures that the school can be reached and the Headteacher contacted at any time. Currently, the head@ account is forwarded directly to the Head's global id account, djr44@chadsgrove.worcs.sch.uk.

10.2. It is recognised that email is not a secure means of communication as messages sent through the Internet use plain, unencrypted text which means that there is potential for them to be intercepted and read. As such, the following methods are used to transfer sensitive and/or confidential data:

- **Egress Switch**
  This secure data exchange process is available to schools in order to transfer files between schools or Local Authority departments
- **School to School (s2s)**
  A national (England) system to transfer pupil and other data between schools and Local Authorities
- **B2B: (Business to Business)**
  A nightly transfer of data from the school SIMS database to the Local Authority ONE System
- **GCSX:** (Government Connect Secure Extranet)
  This system allows officials at local public-sector organizations to interact and share data privately and securely with central government departments, such as the National Health Service, the Criminal Justice Extranet and the Police National Network.
- **COLLECT**
  This website is used to upload School Workforce Census and School Census data to the DfE

10.3. Sensitive or confidential information that cannot be sent using one of the above methods will, instead, be delivered by hand or sent by registered post.

10.4. In order to protect data and the integrity of the school network, users are requested to:

- report any spam or phishing emails to the IT team
- use the school's contacts or address book in order to help stop email being sent to the wrong address.
- be extremely wary of emails requesting or asking for confirmation of any personal information, such as passwords
- take extreme care with emails from unknown senders, particularly where they contain attachments. If in doubt, they should not open the attachments until the identity of the sender has been verified

10.5. Users are also requested not to:

- click on links in unsolicited emails
- email sensitive information unless using one of the systems identified in paragraph 10.2 above
- reply to chain emails.

11. Maintaining a Virus Free Network Environment

11.1. Chadsgrove School recognises the need to ensure that children and young people are safeguarded whilst using ICT and that viruses are an on-going real threat to the stability and integrity of the school network. As such, the following electronic safeguards are in place:

- Smoothwall Internet content filtering
- Sophos anti-virus software (also includes malware protection)
- Sophos email spam filtering
- Sophos email anti-virus scanning

11.2. All staff who use laptops are requested to connect to the school network at regular intervals in order to allow the software to update itself with the identities of the latest viruses.

12. System Updates

12.1. In order to keep the computer operating systems up to date, it is vital that they are regularly updated. To this end Windows Server Updates Service (WSUS) is used. WSUS allows centralised

management of updates for Windows operating systems across the network. It is managed by the CIS technician and points to the Capita IBS servers.

13. Learning Platform

13.1. To gain access to the learning platform, both staff and pupils need to use a user name and password. Once on the platform, access is further restricted depending upon the logon used – for example, pupils can only access their class/home page, whereas members of staff can see all class home pages.

14. Laptop security

14.1. Members of staff who use school laptops as part of their work are requested to:

- shut down the laptop using the shut down or turn off option
- prevent people from watching as passwords are entered
- store their laptop securely
- use a physical laptop lock if this is available in order to prevent theft
- lock the desktop when leaving the laptop unattended

14.2. In addition, they are requested not to:

- leave laptops unattended unless the physical security in place is trusted
- use public wireless hotspots as they are not secure
- let unauthorised people use the laptop
- use hibernate or standby

15. Mobile Storage Devices

15.1. There are three main types of mobile storage devices and staff are advised that none of these should be routinely used for transferring confidential data:

- Memory Cards - The use of memory cards in cameras means that they will generally be used to store photos and video clips of children. It is not normally possible to encrypt this storage media, so the loss of a school digital camera or video camera off site would mean that these images are at the mercy of whoever finds them. In order to minimise the risk of this happening, users are advised to wipe the media as soon as possible after pictures have been taken, once the images have been copied to a secure location
- Memory Sticks - Memory sticks are highly portable, so are easy to lose and steal. The ease of use of these devices can also make it easy for users to transfer viruses from home machines to school
- USB Hard drives – again these are highly portable and so are easy to lose or steal. However, they can be encrypted or password protected so could be used to transfer sensitive or confidential data if this is unavoidable.

16. Non-Windows computers and other devices

16.1. Any computer can be used to store confidential information so the same general considerations regarding care with transfer of data, encryption, transporting devices, viruses, etc., apply as described in this policy.

17. Apple Mac desktop computers and laptops

17.1. Apple computers (including iMacs and MacBooks) run the Mac OS operating system, and are frequently thought to be less vulnerable to viruses than their Windows PC equivalents. However, Mac viruses do exist, and the Sophos for Mac is used to protect them.

18. Tablet Computers (including iPad, iPod and Android devices)

18.1. Staff are advised to remove any images on tablet devices as soon as possible and transfer these to secure storage on the server.

19. Personal Data Stored Electronically

19.1. Personal data is stored on administration machines in the school office and the Head Teacher's office. These machines are encrypted and the rooms that they are in are locked when the school is closed. Databases such as SIMS are also protected by additional password security.

19.2. Some personal data, for example, pupil annual review documentation is held on the curriculum server but is only accessible to members of staff using their personal logons. This level of accessibility is necessary for staff to be able to fully execute their duties and responsibilities as teachers.

19.3. Personal data is held for the times specified by the records management society and more details on this issue can be found in the Data Protection policy.

20. Personal Data Not Stored Electronically

20.1. Personal data, as well as being stored electronically, also continues to be held in paper form at Chadsgrove School. Such data includes:

- Pupil records
- Staff records
- Medical records
- Pupil Information Folders
- Information regarding the safeguarding of pupils

20.2. With the exception of Pupil Information Folders which are stored in classrooms for ease of access by teaching staff, all personal information is stored in the school office, Headteacher's office, Nurse's office or offices belonging to members of the Senior Leadership Team. Each of these rooms is locked when the school is closed.

20.3. Pupil and staff records are all stored in locked filing cabinets, access to which is restricted to members of staff who have been issued with a key or who have been authorised to access the information using one of those keys. Three sets of keys are available – one is held by the Head Teacher, one by the School Business Manager and the third by the office administrator. Keys to medical records held in the school nurses room are held by the school nurse and pupil care plans are stored in a locked room accessible by the Medications Manager or other authorised members of staff.

20.4. Personal or sensitive data that is held in paper form is disposed of using a secure, on-site, shredding service.

21. Data Losses

21.1. Staff are required to report any data losses to the Head Teacher as soon as they become aware of the loss. If the data loss is of a personal nature (i.e. covered by the Data Protection Act) then the Head Teacher will liaise with the Information Commissioners office.

22. Monitoring

22.1. Staff and pupil use of computers and the school network is monitored by Deb Rattley (Headteacher) and Angela Macvie (Deputy Headteacher) using Policy Central Enterprise – a system capable of monitoring computer use and ensuring that anything that falls outside of the school's Acceptable Use Policy is captured on a database and can be followed up by senior staff as necessary. More information on this can be found in the E-Safety and Acceptable Use Policy.

23. Social Networking

23.1. Social networking is a fact of life for staff and pupils; all users need to be aware of the benefits and dangers inherent in the use of these systems, while understanding that they need to manage the information that they make available to the public.

23.2. Staff are requested to ensure that they:

- take charge of their digital reputation and do not bring their professional status or the school into disrepute
- do not inadvertently make their personal information available to pupils (or their parents)
- remain in control of how public their digital information is by applying individual site privacy settings
- never enter personal identifiable information on social networking sites
- use strong passwords and logins to prevent their site from being misused

24. Sharing information with overseas schools

24.1. Should Chadsgrove want to share information with overseas schools there is an acknowledgement of the need to be aware that their e-safety regulations may not be as rigorous as those in the UK. As such, sharing personal data outside of the European Economic Area is only permissible if that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to processing personal data. If in any doubt a teacher should refer any issues of this nature to the Head Teacher for an appropriate decision to be made.

25. Cloud data storage, applications and security

25.1. Over recent years, it has become common for suppliers to offer data storage facilities through internet sites and many computer applications have become available that essentially run remotely via a web browser. This has become known as "cloud computing". Chadsgrove School currently uses the following cloud applications:

- Dropbox data storage
- Microsoft OneDrive
- School website and learning platform
- B Squared
- WriteOnline
- RM Maths

25.2. Any cloud services that are used are based in the European Economic Area in order to comply with the Data Protection Act (1998).

25.3. Data on cloud applications is only available to those with an appropriate logon username and password.

26. Secure disposal of equipment

26.1. Equipment is disposed of in the following ways:

- **Networked curriculum computers**
  These do not contain any user data so are reformatted/recycled as appropriate.
- **Networked admin computers and associated data storage devices**
  In many cases these will contain user data, some of which may be confidential so the hard drives on these machines are securely destroyed and then the equipment is recycled as appropriate.
- **Curriculum servers and associated data storage devices**
  These may contain staff shared data and staff user accounts so the hard drives on these machines are securely destroyed and then the equipment recycled as appropriate.
- **Admin servers and associated data storage devices**
  These will contain confidential data so the hard drives on these machines are securely destroyed and then the equipment is recycled as appropriate.
- **Teachers' laptops drives**
  In many cases these will have been used to store confidential information so the hard drives are securely destroyed and then the equipment recycled as appropriate.

26.2. Collection, secure destruction and the recycling of computers that are no longer required is carried out by a third party company and a certificate of data destruction obtained.

27. Disciplinary and Related Action

27.1. Chadsgrove School wishes to promote the highest standards in relation to good practice and security in the use of data. Consequently, it expects and supports the integrity of its staff.

27.2. Disciplinary procedures will be instigated if there is evidence to suggest that employees are disregarding information and data security procedures and, in exceptional circumstances where there are reasonable grounds to suspect that an employee has committed a serious criminal offence, the police will be informed and a criminal prosecution may follow.

28. Acknowledgements

28.1. Material in this document is adapted from the following documents:

- Becta ICT Advice document “Data Protection and Security, a summary for schools” (2004).
- Capita IBS Schools document “System and Data security’ (2009)
- Data Handling Procedures in Government (2008)
- South West Grid for Learning E-Safety School Template Policies (2013)

28.2. The Copyright of these documents is held by their relevant authors and their use is gratefully acknowledged.

Appendices

1. Back Up Procedures
2. Password policy

Appendix 1 – Back Up Procedures

Chadsgrove Curriculum Server – including pupil and staff personal storage areas
Daily automatic backups. This back up procedure is monitored by the school ICT technician.

Chadsgrove Media Server – images, videos and sound files
Saved onto the 'old' server and further backed up onto a QNAP NAS drive. This back up procedure is monitored by the CIS technician.

SIMS / MIS Data (Office 'K' Drive)
SIMS is centrally hosted by the Local Authority. As such it is automatically backed up by the Local Authority using a corporate back up facility.

SAP
SAP is centrally hosted by the Local Authority. As such, it is automatically backed up by the Local Authority using a corporate back up facility. Unlike SIMS, no other files need to be backed up in school; everything is dealt with by the Local Authority. This back up is monitored by the Local Authority.. The password for SAP is changed every 2 months.

PFP (Office 'T' Drive)
PFP is no longer used. However, records retention procedures dictate that this information still needs to be retained. As such, a back up of the drive has been made on to a memory stick and this is stored in a locked cabinet in the school office.

Other Office Documents
Other office documents are stored on the curriculum server and, as such, they are backed up using the curriculum server procedures.

Outreach Data
Manual backups of any data not held on the curriculum server are made to USB flash drives on a termly basis. One back up is stored in a locked cabinet and the other in a fire proof box. This back up is performed by the Outreach Administrator.

BSquared
Daily back up at on off site location, hosted by B Squared

Appendix 2 - Password Policy

Access to the School Network and to data stored on it is controlled by usernames and passwords. Special database programs, such as the SIMS system, have separate access controls in addition to this.

User names and passwords must never be communicated to any other person, nor should any person log in to the network for another person. This could result in unauthorised access to information.

Network passwords must:

- Be 8 or more characters in length
- Contain numbers as well as letter
- Contain symbols or non alpha-numeric characters
- Not be easily guessable
- Be reasonable to type – staff should have to resort to writing them down

The network will force the user to choose a new password at least annually.

Passwords must also be changed if the user thinks that a password may have been compromised

It is not good practice to use the same password for all applications, though it can be sensible to have a small number of passwords in use at any time.

Do Not:

- Share your passwords with anyone else
- Write your passwords down
- Use your work passwords for your own personal on-line accounts
- Save passwords in web browsers if offered to do so
- Use your user name as a password
- Use names as passwords
- Email your password or share it in an instant message