School Systems and Data Security Policy

March 2020

Policy No: 85

DATE APPROVED BY GOVERNING BODY: 4/3/2020

DATE OF NEXT REVIEW: March 2021

LEAD: Angela Macvie

CONTENTS

School Systems and Data Security Policy Details

Teacher Responsible: Mrs Angela Macvie

Data Controller: Chadsgrove School (Deb Rattley)

Data Protection Officer (Main School): Mr Mark Loveday

Data Protection Officer (Teaching School and 19-25): Mrs Angela Macvie

Strategic ICT Lead: Mrs Angela Macvie

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.

1.2. Chadsgrove also deals with large quantities of information that is not regarded as personal in terms of the General Data Protection Regulations (EU) 2016/679 (GDPR) and the Data Protection Act 2018 but nevertheless is important to the smooth running of the school.

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

1.4. 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.

1.5. Chadsgrove will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. Where the school needs to share personal data with a third party, it carries out due diligence and takes reasonable steps to ensure that it is stored securely and adequately protected.

1.6. This policy applies to all staff employed by Chadsgrove School, and to external organisations or individuals working on the school's behalf.

2. Aims

2.1. The policy aims to ensure that:

- All personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulations (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018).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 both information and ICT security and their own responsibilities in this respect

3. Roles and Responsibilities

3.1. The **Governing Body** has overall responsibility for ensuring that Chadsgrove School complies with all relevant data protection and security obligations

3.2. The **Head Teacher** acts as the representative of the data controller, for the purposes of data protection. She is also responsible for working with the Governing Body to ensure that Chadsgrove complies with all relevant data protection and security obligations

3.3. The **Data Protection Officers** are responsible for

- Monitoring the school's compliance with data protection law and developing related policies and guidelines where applicable.
- Providing an annual report of their activities directly to the Governing Body and, where relevant, reporting to the Governing Body their advice and recommendations on school data protection issues.
- Being the first point of contact for individuals whose data the school processes, and for the ICO.

3.4. All **school staff** are responsible for:

- Taking good care of any equipment provided to them to protect from loss or theft
- Setting and maintaining strong passwords
- Reading and taking responsibility for the contents of this policy
- Ensuring that paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept secure when not in use
- Ensuring that papers containing confidential personal data are not left on office and classroom desks, on staffroom tables, or anywhere else where there is general access
- Collecting, storing and processing any personal data in accordance with the Data Protection Policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the Data Protection Officers in the following circumstances:
  - ❖ With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - ❖ If they have any concerns that this policy is not being followed
  - ❖ If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - ❖ If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual or transfer personal data internationally
  - ❖ If there has been a data breach
  - ❖ Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
  - ❖ If they need help with any contracts or sharing personal data with third parties.

4. Physical Security

4.1. 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 lockable room with no direct entry from the outside
- The server is in a secure, 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 Head Teachers 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 networked computer as soon as possible in order to minimise the risk of loss The files should then be deleted from the mobile device

5. Logical Security

5.1. Logical security is about ensuring the protection of information by protecting computer files using the following methods:

Encryption

5.2. 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.

5.3. 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 Netbuilder technician, as adequate technical solutions are not yet available. Instead the server is protected by physical security as it is kept in a locked cabinet.

5.4. School staff are advised not to use memory sticks to store personal or sensitive information. There should be no need to place personal data on memory sticks in order to work on documents outside of school as secure, remote access to the school server is provided to authenticated users. If this is unavoidable, for whatever reason, the use of external hard drives that are password protected is advised.

Network Access Restrictions

5.5. 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:

5.6. In addition:

- All users must log on and staff are required to provide a password as they are able to access sensitive data such as Annual Review information.
- 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.
- Users are not able to install or uninstall software. This reduces the risk of a computer becoming corrupted or infected with viruses etc.
- 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.
- 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.

5.7. In order to manage the network, Chadsgrove uses Windows Group Policy in conjunction with Windows Server 2012. Group policies are managed by the Netbuilder technician in liaison with the 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.

5.8. In addition, in order to create a manageable and secure school network, a range of management tools are available to the network administrators (Netbuilder technician and members of the ICT/Computing Team) in order to simplify tasks such as:

- Managing users – creating or modifying users and setting passwords quickly and easily
- 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 Netbuilder technician having to visit every computer
- Managing computers so that the Netbuilder technician can rebuild corrupted machines quickly and easily, using a standard setup

Back Up Procedures

5.9. 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 to an external back up drive and to an external 'Cloud' backup, supplied and maintained by Netbuilder
- Media Servers – saved onto the 'old' curriculum server with a weekly automatic back up to a QNAP NAS drive and to an
- Office, Outreach and School2School Support Data– backed up daily along with the main server onto an external back up device and to an external 'Cloud' backup, supplied and maintained by Netbuilder
- ScholarPack – hosted and backed up by supplier
- CPOMS – hosted and backed up by supplier
- SOLAR – hosted and backed up by supplier
- RM Maths – hosted and backed up by supplier

- Lexia – hosted and backed up by supplier
- Mercury Finance – hosted and backed up by supplier

5.10. No data is stored on the hard drives of any machines that are permanently 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 2018), for example, lesson resources, on the hard drive of their laptops. However, they then become responsible for backing up that data on to a suitable external device, the school network or other media.

5.11. Half Termly tests and weekly reviews of backup procedures take place. These are performed by the Netbuilder technician during his weekly visit to the school in liaison with the strategic ICT lead.

Passwords

5.12. Passwords are integral to data security at Chadsgrove. Staff are made aware of the password policy (see Appendix 1) 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
- passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices
- staff and pupils are reminded that they should not reuse passwords from other sites and should change their passwords at regular intervals

5.13. 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.

5.14. 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 with the same name repeated as the password, No confidential/personal data is stored on any network spaces that pupils are able to access.

5.15. 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).

5.16. Any files downloaded to computers are set to automatically delete at the start of each month.

6. Procedural security

6.1. 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 the School Information Management System (ScholarPack, which contains student and staff personal data), Mercury (financial information) and office-based data are restricted to specific machines or to specific individuals through user names and passwords.
- Administrative machines in the school office are not accessible from other machines in school unless a link has been specifically 'mapped' to them the Netbuilder 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.

7. Photographs and Videos

7.1. As part of school activities, staff may take photographs and record images of individuals within the school.

7.2. The school obtains written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. How the photographs and/or videos will be used will be clearly explained to both the parent/carer and, where appropriate, the pupil.

7.3. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, Chadsgrove asks that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

7.4. Uses of photographs and videos may include:

- Within school on notice boards and in school magazines, brochures, newsletters, communication aids etc.
- Within school for assessment purposes
- Outside of school by external agencies such as the school photographer, or newspapers
- Online on the school website or social media pages.

7.5. Consent can be refused or withdrawn at any time. If consent is withdrawn, the school will delete any photographs and videos and not distribute them further.

7.6. When using photographs and videos, outside of classroom areas, the school will not accompany them with any other personal information about the child, in order to ensure they cannot be identified.

7.7. Occasionally, school staff may use images/videos as part of training materials delivered to outside agencies. Consent, from parents/carers, will always be sought before such materials are used.

8. School WI-FI Security

8.1. 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 Netbuilder. The network was professionally installed and is maintained, as necessary, by Netbuilder.

9. Email, Messaging and Secure Communication

9.1. Chadsgrove uses standard mailbox and domain names, for example, office@chadsgrove.worcs.sch.uk which conform to national standards. This ensures that the school can be reached and the Head Teacher contacted at any time. Currently, the head@ account is forwarded directly to the Head's personal account, djr44@chadsgrove.worcs.sch.uk.

9.2. 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
- **GCSX:** (Government Connect Secure Extranet)
  This system allows officials at local public-sector organisations 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
- **Worcesteshire County Council Secure Communication Portal**
  This is used to communicate sensitive/confidential information with the Local Authority and is accessed via two factor authentication

9.3. 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.

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

- Report any spam or phishing emails to the ICT/Computing 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

9.5. Users are also requested not to:
- Click on links in unsolicited emails
- Email sensitive information unless using one of the systems identified in paragraph 9.2 above
- Reply to chain emails.

10. Maintaining a Virus Free Network Environment

10.1. Chadsgrove recognises 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:
- Internet content filtering provided by Netbuilder as part of their broadband service
- Windows Defender anti-virus software provided as part of the Office 365 subscription and maintained by Netbuilder

10.2. 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.

11. System Updates

11.1. 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 Netbuilder technician.

12. Learning Platform

12.1. 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.

13. Laptop and Tablet Security

13.1. 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

13.2. 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

14. Mobile Storage Devices

14.1. 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 on the school network

- **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 External 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 data if this is absolutely unavoidable

15. Personal Data Stored Electronically

15.1. Personal data, for example the Single Central Record, is accessed via administration machines in the school office. These machines are in a room that is locked when the school is closed. Databases such as ScholarPack, CPOMS and Mercury are also protected by additional password security.

15.2. 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.

15.3. 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.

16. Personal Data Not Stored Electronically

16.1. 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

16.2. 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, Head Teacher's office, Nurse's office or offices belonging to members of the Senior Leadership Team. All information is held in locked cupboards and most rooms are also able to be locked when the school is closed.

16.3. 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 meds manager or other authorised members of staff.

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

17. Data Losses

17.1. 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 Data Protection Officer will liaise with the Information Commissioners Office.

18. Monitoring

18.1. Staff and pupil use of computers and the school network is monitored by Deb Rattley (Head Teacher) and Angela Macvie (Deputy Head Teacher) using Future Cloud – 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 Online Safety and Acceptable Use Policy.

19. Social Networking

19.1. 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.

19.2. 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
- Do not become 'friends' with or 'follow' pupils or their parents, even after they have left the school.

Further information with regard to this subject can be found in the Staff Code of Conduct (September 2017)

20. Sharing Information with Overseas Schools

20.1. Should Chadsgrove want to share information with overseas schools there is an acknowledgement of the need to be aware that their online 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.

21. Cloud Data Storage, Applications and Security

21.1. 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 currently uses the following cloud applications:

- Microsoft Office 365
- E-Schools website and learning platform
- SOLAR
- CPOMS
- ScholarPack
- WriteOnline
- RM Maths
- Lexia
- Mercury Finance

21.2. Any cloud services that are used are based in the European Economic Area in order to comply with the Data Protection Act (2018).

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

22. Secure Disposal of Equipment and Data

22.1. 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.

22.2. The 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.

22.3. Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where it is not possible or there is no need to rectify or update it.

22.4. Chadsgrove will shred paper-based records and delete electronic files. The school may also use a third party (currently Shred-it) to safely dispose of records on the school's behalf. If this occurs, the school will require the third party to provide sufficient guarantees that it complies with data protection law.

22.5. Secure storage bins are available for documents waiting to be shredded. Should these become full, excess materials are stored in the locked archive store.

23. Disciplinary and Related Action

23.1. 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.

23.2. 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.

24. Monitoring and Review

24.1. The Head Teacher, Angela Macvie and Netbuilder monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

24.2. This policy will be reviewed every two years.

24.3. The governing board is responsible for approving this policy.

25. Linked Policies

- Freedom of Information (Policy Number 86)
- Data Protection (Policy Number 84)
- Staff Code of Conduct (Policy Number 100)
- Safeguarding Children (Policy Number 73)

Appendix 1 - Password Policy

Access to the School Network and to data stored on it is controlled by usernames and passwords. Special database programs, such as Local Authority Secure Communications, 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