

THE DOVE-SHELL FEDERATION

East Crompton St James' CE (VA) Primary School

St Thomas' Moorside CE (VA) Primary School



SCHOOL SYSTEMS AND DATA SECURITY POLICY

Date of Policy / Reviews	Author(s)	Approved by Gov. Body	Signed	Date for review
17/10/2019	Deborah Hawkins			

Introduction

The Dove-Shell Federation collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered to enable us to educate the children and under GDPR guidelines, to comply with a legal obligation, to perform an official task in the public interest or to protect the individual's vital interests.

This policy deals with how computer systems and the information stored within them are kept safe and secure. It also addresses how data how all other data that is not electronic is stored safely and securely.

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.

Separate policies are available that deal with Data Protection, GDPR and Freedom of Information.

Physical Security

Physical security is about ensuring the protection of information by storing it securely and restricting access to it. The Dove-Shell Federation 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 classroom computers are stored in lockable cabinets.
- The servers are in a locked cabinet
- All administration machines that hold personal data are in rooms that are locked when school is closed and that have electronic access locks that can only be opened by authorised staff members.
- The files of pupils who are currently on roll are stored in lockable cabinets in the school office.
- The files of pupils who have left and any other confidential information that needs to be retained are stored in locked cupboards.

Logical Security

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

- Encryption – to prevent unauthorised access to data.
- Network access restrictions – to ensure that users only see the information they are authorised to access.
- Backup procedures – to ensure that any lost data can be retrieved.

- Passwords – to prevent unauthorised access to sensitive or confidential data.

Procedural Security

Procedural security is about ensuring 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), FMS (financial information), CPOMS (safeguarding information) and Target Tracker (assessment data) are restricted to certain users and data levels by usernames and passwords.
- Administrative machines in the school office operate on their own network that is not accessible from other machines in school unless mapped by Ranatech and this can only be done with authorisation from the Headteacher.
- 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.

Encryption

Encryption is a process whereby the data held on a computer is encoded so 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.

Any computers or laptops that may be removed (or stolen) from the school and that contain sensitive data are encrypted.

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 are advised.

Networks

Google drives are used to restrict access to all information. Staff have their own google drive and are then given access to the shared drives that they are authorised to view. Most people are only granted access to the subject resources drive and the teacher shared planning drive.

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 access every computer.
- Managing computers so the technician can rebuild corrupted machines quickly and easily, using a standard setup.

Backup Procedures

In order to ensure information can be retrieved in the event of a loss, the following back up procedures take place using scheduled systems:

Data is backed up and stored in a cloud based system on a daily basis.

A full data and software backup is taken every day onto a USB stick that is kept with the server.

Data should not be stored on the hard drives of any machines that are connected to the school network as they are not backed up. Users should only store work documents on their google drive. If they have their own non work related information on their laptop, they are responsible for creating their own backup onto an external device or storage media.

Passwords

Passwords are integral to data security within the Dove-Shell Federation. 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-alphanumeric characters.
- Are easy to remember, but hard to guess.
- Are reasonable to type – staff should not have to resort to writing them down.

Staff are requested not to:-

- Save passwords in web browsers if offered to do so.
- Use usernames as passwords.
- Email passwords or share them in an instant message.

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.

School WI-FI Security

The Dove-Shell Federation 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.

E-Mail, Messaging and Secure Communication

The Dove-Shell Federation use First Class for their email system which is hosted by Oldham Council. Messages sent to other first class email addresses are encrypted.

It is recognised the emails to non-First Class addresses is not a secure means of communication as messages sent though the Internet use plain, unencrypted text which means 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 system to transfer pupil and other data between schools, Local Authorities, upload workforce census and school census data.
- **CPOMS** – This software is used to transfer sensitive data such as Safeguarding and SEN details to a receiving school if they also have the software.

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.

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

- Report any spam or phishing emails to the Local Authority IT Team (usually Jonathan Howarth).
- Use the First Class address book or the school files to ensure emails are not sent to the wrong address.
- Be extremely wary of emails requesting or asking for confirmation of any personal information, including 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.

Users are also requested not to:-

- Click on links in unsolicited emails.
- Email sensitive information unless using one of the systems above or First Class address to First Class address.
- Reply to or forward chain emails.

Maintaining a Virus Free Network Environment

The Dove-Shell Federation recognise the need to ensure children and young people are safeguarded whilst using ICT and that viruses are an ongoing real threat to the stability and integrity of the school network. As such, the following electronic safeguards are in place:-

- Panda anti-virus software (also includes malware protection).
- Email spam filtering.
- Email anti-virus scanning.

All staff using laptops are requested to run software updates for the anti-virus software when requested.

System Updates

Staff are reminded to allow their laptops to run updates at regular intervals, they should get a prompt when updates are available.

DB Primary

To gain access to DB Primary, both staff and pupils need to use a username and password. Once on DB Primary, access is further restricted depending on the logon used, for example, pupils can only access their class/home page, whereas members of staff can see all class home pages.

CPOMS

Access is granted by usernames and passwords, staff members have access to the class they work with but no other classes. They can input information and view alerts but cannot look back through previous information.

SLT and SENCOs have access to the whole system which they access via usernames and passwords and also a meriloc key.

Laptop Security

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

- Shutdown the laptop using the shut down or turn off option (not just by closing the top).
- Prevent people from watching as passwords are entered.
- Store their laptop securely.
- Lock the desktop when leaving the laptop unattended.

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.

Mobile Storage Devices

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 they will generally be used to store photos and video clips of children. It is not normally possible to encrypt this storage media which means the loss of a school digital camera or video camera off site would mean these images could be viewed and used by the person that finds them. To minimise the risk of this, users are advised to wipe the media as soon as possible after pictures have been taken and copied to a secure location.
- Memory sticks – Memory sticks are highly portable so are easy to lose or steal. The ease of use with 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.

Non-Windows computers and other Devices

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.

Tablet Computers (including iPad, iPod and Android devices)

As tablet computers are portable and easily lost or stolen, staff are advised to remove any images as soon as possible and transfer them to secure storage on the google drive.

Personal Data stored Electronically

Personal data is stored on administration machines in the school office and the Head teacher's office. These offices are locked when the school is closed and access is only granted to certain people with a security badge for the electronic lock.

Personal data is held for the times specified by the records management policy.

Personal Data not Stored Electronically

Personal data, as well as being stored electronically, also continues to be held on paper form. Such data includes:-

- Pupil records.
- Staff records.
- Medical records.
- SEN files.

Pupil and Staff records are all stored in locked 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 the keys. Three sets of keys are available, one is held by the Assistant Head, one by the Business Manager and the third by the School Administrator. Keys for the SENCO cabinet have been issued to the SENCO, Assistant Head and the office (which is kept in the safe).

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

Data Losses

Staff are required to report any data losses to the Headteacher 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 or GDPR Guidelines) the Headteacher will liaise with the Information Commissioners Office (ICO).

Monitoring

Staff and pupil use of computers and the school network is monitored by Ranatech, ensuring that anything that falls outside of the school's Acceptable Use Policy is captured 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.

Social Networking

Social networking is part of everyday life for staff and pupils, all users need to be aware of the benefits and dangers in the use of these systems, whilst understanding the need to manage information they make available to the public.

Staff are requested to ensure 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.

Sharing Information with Overseas Schools

Should school want to share information with overseas schools there is an acknowledgement of the need to be aware 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.

Cloud Data Storage

Over recent years, it has become common for suppliers to offer data storage facilities through internet sites and many computer applications have become available the essentially run remotely via a web browser. This has become known as cloud computing. The Dove-Shell Federation currently use the following applications:-

- Google drive.
- DB Primary.
- School Website.
- Parent Mail.
- Parent Pay.
- Target Tracker.
- CPOMS.
- Teachers 2 Parents.
- Learning Book.

Any cloud services that are used are based in the European Economic Area in order to comply with the Data Protection Act and GDPR Guidelines.

Data on cloud applications is only available to those with a username and password.

Secure Disposal of Equipment

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 destruction is obtained.

Disciplinary and Related Action

The Dove-Shell Federation wishes to promote the highest standards in relation to good practice and security in the use of data. Consequently, we expect and support the integrity of our staff.

Disciplinary procedures will be instigated if there is evidence to suggest that employees are disregarding information and data security procedures.

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 SIMS, have separate access controls in addition to this.

Usernames 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 letters.
- Contain symbols or non-alphanumeric characters.
- Not be easily guessed.
- Be reasonable to type – staff should not have to resort to writing them down.

The network will force the user to choose a new password regularly.

Passwords must also be changed if the user thinks 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 you password or share it in an instant message.