Springmead School

Date 27/04/18

INFORMATION SECURITY POLICY

This is a whole school policy including EYFS and is audited regularly using 360 Degree Safe and 360 Degree Data

Introduction

All School staff shall do everything within their power to ensure confidentiality and security of all information. The loss of or unauthorised access to School's data, including personal data, is likely to cause harm to pupils, parents or staff and may result in relevant authorities taking enforcement action.

1. Purpose

1.1. The School is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.

1.2. The School collects and maintains its pupils, pupil's parents and guardians, employees, and other information for the purpose of providing education services.

1.3. All School employees have a duty to process all information in a professional, responsible, ethical, and legal manner, consistent with this Policy at all times.

1.4. The purpose of this Policy is to provide a framework which will assist the School to:

1.4.1. protect against potential breaches of confidentiality;

1.4.2. ensure all our information assets and IT facilities are protected against damage, loss or misuse;

1.4.3. support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and

1.4.4. increase awareness and understanding in the School of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they themselves handle.

2. Scope

2.1. The Policy applies to all staff, which for these purposes includes teachers, temporary and agency workers, volunteers, placement students and any other contracted staff such as administration or support staff who interact with information held by the School and the information assets and IT facilities used to store and process such information.

2.2. The information covered by the Policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the School, in whatever media. This includes information held on computer systems, mobile devices, phones, paper records, and information transmitted orally.

2.3. All staff must be familiar with this Policy and comply with its terms.

2.4. This Policy supplements School other policies relating to *data protection and online safety*

2.5. The School may supplement or amend this Policy by additional policies and guidelines from time to time. Any new or modified Policy will be circulated to staff before being adopted.

3. Information Security Governance

3.1. The Principal is responsible for the monitoring and implementation of this Policy. If you have any questions about the content of this Policy or other comments you should contact the School Principal.

4. General Principles

4.1. All School information must be treated as confidential and be protected from loss, theft, misuse or inappropriate access or disclosure.
4.2. Staff should discuss with the Deputy Principal the appropriate security arrangements which are appropriate and in place for the type of information they access in the course of their work.
4.3. Staff should ensure they attend any information security training they are invited to.
4.4. Information is owned by the School and not by any individual member of staff or team.
4.5. The School will hold the minimum information necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for.
4.6. Staff must ensure that data held is accurate and that inaccuracies are corrected without unnecessary delay. Any inaccuracies discovered should be notified to the Deputy Principal immediately.
4.7. All confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as the need for its retention has passed. You should not retain any information for longer than is required, if you are uncertain about whether or not you should still hold information then please contact the Deputy Principal immediately.

5. Access to School premises and information

Note: School to update this section to reflect physical security measures that are in place.

5.1. Security precautions must be taken by all staff. Please refer to [insert Physical Security Policy title] for further guidance.
5.2. Documents containing confidential information, including personal data and equipment displaying confidential information should be positioned in a way to avoid them being viewed by people passing by, e.g. through office windows.
5.3. Staff should take adequate steps and regularly review the physical security of buildings and ensure that only authorised persons have an access to storage systems containing information.
5.4. At the end of each day, or when desks are unoccupied, all paper documents, backup systems and devices containing confidential information must be securely locked away.
5.5. All mobile devices should be kept as securely as possible on and off the School premises. If they contain personal information they should be under lock and key when not in use.

6. COMPUTERS AND IT

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It also needs to ensure that the relevant people will be effective in carrying out their Online Safety responsibilities.

- School ICT systems are managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage agreement
- There are regular reviews and audits of the safety and security of school ICT systems
- Servers are securely located and physical access is restricted.
- All users have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users are recorded by the Bursar and are reviewed, at least annually.
- All users, at KS2 and above, are provided with a username and password. An up to date record of users and their usernames is kept on the server. Users are required to change their password every 90 days.
- The "administrator" level passwords for the school ICT system, can be used by Matt Stephenson, The computing lead and the Bursar and must also be available to the Principal and Deputy Principal and kept in a secure place. Site documentation is held off site by our ICT Consultant Mattt Stephenson.
- Users are made responsible for the security of their username and password, they must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to our Online Safety Coordinator or Deputy Principal.
- The school has provided enhanced user-level filtering through the use of the Smoothwall filtering software.
- In the event of a need to switch off the filtering for any reason, or for any user, this is logged and carried out by a process that is agreed by the Principal or Deputy Principal.
- Staff have access to all sites. Their internet access is monitored.
- Requests from staff for sites to be removed from the 'student filtering' will be considered by the Online Safety Committee and actioned by Matt.
- School staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this monitoring by screen prompt when logging on.
- An appropriate system is in place for users to report any actual / potential Online Safety incident to the Committee. Do we need to display the system in classes etc? There is a log book available that lists Online safety incidents.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system. The Guest log is monitored by the Bursar.
- An agreed policy is in place (to be described) regarding the downloading of executable files by users
- An agreed policy for Holiday club to only use a holiday club log in during opening hours. Children would not use their school log in. The children would have restricted use of sites to ensure E- safety during the session. This password would be changed on the last day of holiday club as part of the tidying teams.

- An agreed policy is in place (See below) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school workstations / portable devices. (see School Personal Data Policy Template in the appendix for further detail)

6.1. All staff shall use password protection and encryption where it is prescribed by IT teams to maintain confidentiality.
6.2. Strong passwords, i.e. at least eight characters long and containing special symbols, shall be used.
6.3. Confidential information must not be copied onto removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of the [insert relevant department or role holder] and even then it must be encrypted. Data copied onto any of these devices should be deleted as soon as possible and stored on the School's computer network in order for it to be backed up.
6.4. All electronic data must be securely backed up at the end of each working day.
6.5. Staff should ensure they do not introduce viruses or malicious code on to Schools' systems. Software should not be installed or downloaded from the internet without it first being virus checked. Staff should contact [insert role holder or department, e.g. IT Manager or IT department] for guidance on appropriate steps to be taken to ensure compliance.
6.6. Staff should be careful when accessing School information outside of the School in particular be aware of the risks of using publicly available Wi-Fi and using devices in public places.
6.7. Staff must not download or install any applications or software onto School devices without the express written consent of [insert role holder or department, e.g. IT Manager or IT department].

7. Communications and transfer

7.1. Staff should be careful about maintaining confidentiality when speaking in public places.
7.2. Confidential information should be marked 'confidential' and circulated only to those who need to know the information in the course of their work in the School.

7.3. Confidential information must not be removed from the School's premises without permission from [*insert relevant role holder or department*] except where that removal is temporary and necessary.

7.4. In the limited circumstances when confidential information is permitted to be removed from the School premises, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. Staff must ensure that confidential information is:

7.4.1. not transported in see-through or other un-secured bags or cases;

7.4.2. not read in public places (e.g. waiting rooms, cafes, trains);

7.4.3. not left unattended or in any place where it is at risk (e.g. in conference rooms, car boots, cafes).

7.5. Postal, document exchange (DX), fax and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.

7.6. All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.

7.7. Sensitive or particularly confidential information should not be sent by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

8. Home working

8.1. Staff shall not take confidential or other information home without the permission of the [*insert relevant role holder or department*] and only do so where satisfied appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information.

8.2. In the limited circumstances in which staff are permitted to take School's information home, staff must ensure that:

8.2.1. confidential information must be kept in a secure and locked; and environment where it cannot be accessed by family members or visitors;

8.2.2. all confidential material that requires disposal must be shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed.

9. Transfer to third parties

9.1. Third parties should only be used to process School information in circumstances where written agreements are in place ensuring that those service providers offer appropriate confidentiality, information security and data protection undertakings.

9.2. Staff involved in setting up new arrangements with third parties or altering existing arrangements should consult the [*insert relevant role holder or department*] for more information.

10. Overseas transfer

10.1. There are restrictions on international transfers of personal data. Staff must not transfer personal data internationally at all OR outside the EEA (which includes the EU member states, Iceland, Liechtenstein and Norway) without first consulting the [*insert relevant department or role holder*].

11. Reporting breaches

11.1. All staff have an obligation to report actual or potential data protection compliance failures to the Deputy Principal. This allows the School to:

11.1.1. investigate the failure and take remedial steps if necessary; and

11.1.2. make any applicable notifications.

12. Consequences of failing to comply

12.1. The School takes compliance with this Policy very seriously. Failure to comply puts pupils, staff and the School at risk. The importance of this Policy means that failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

Staff with any questions or concerns about anything in this Policy should not hesitate to contact the Principal.

Monitoring and review

This policy is the principal's on going responsibility and its effectiveness will be reviewed annually in consultation with the staff.

Signed:

Date: