SCHOOL INFORMATION SECURITY POLICY

Fourlanesend C P School

September 2022

Suggestions for use

The School shall carefully review this template and update sections accurately to reflect existing practises.

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. Fourlanesend C P School is committed to the highest standards of information security and treats confidentiality and data security extremely seriously.
1.2. Fourlanesend C P 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:
  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 school governors, teachers, temporary and agency workers, volunteers, placement students and any other contracted staff such as administration or support staff.
2.2. The information covered by the Policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of Fourlanesend C P 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 Schools' other policies relating to data protection, email, fax and Internet, document retention.
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 data protection governor (Piers Taylor) 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 data protection governor.

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 Rebecca Norton 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 unless otherwise agreed by Rebecca Norton.
4.4. Information is owned by the School and not by any individual 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.
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 – see retention policy for details.

5. Access to school premises and information

5.1. Security precautions must be taken by all staff. Please refer to Data Protection Policy 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

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. Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords should not be written down or given to others.

6.4. Confidential information must not be copied onto removable hard drive, CD or DVD or memory stick/ thumb drive without the express permission of Rebecca Norton 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.
6.5. All electronic data must be securely backed up at the end of each working day.
6.6. 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 Rebecca Norton for guidance on appropriate steps to be taken to ensure compliance.

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 Rebecca Norton 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. Only transported in locked boxes provided;
  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 sent by email containing confidential warning (see Rebecca Norton for details) or be sent by tracked DX or recorded delivery.

8. Home working

8.1. Staff shall not take confidential or other information home without the permission of Rebecca Norton 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 in the box provided; 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 Company 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 Rebecca Norton for more information.

10. Overseas transfer

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 Rebecca Norton.

11. Reporting breaches

11.1. All staff have an obligation to report actual or potential data protection compliance failures to Rebecca Norton or Piers Taylor. 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. Fourlanesend C P 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 Rebecca Norton or Piers Taylor.