Information Security Policy

St John's School
LEATHERHEAD

Date of issue:	28 March 2018, last update September 2020
Date of next review:	August 2022
Responsible person:	IT Network Manager
Approved by:	Operations and Compliance Director
References:	Data Protection Policy and Compliance Procedures for Staff (L19) Privacy Notices for Staff, Pupils, Parents and Alumni Staff Conduct Policy (7E)
Policy Number:	L5

Introduction

1. Information security is about what you and the School should be doing to make sure that Personal Data is kept safe. This is the most important area of data protection to get right. Most of the data protection fines have come about because of information security breaches.

2. This policy should be read alongside the School's Data Protection Policy and Compliance Procedures which gives an overview of your and the School's obligations around data protection. The School's Data Protection Policy and Compliance Procedures can be found on SharePoint. In addition to the Data Protection Policy and Compliance Procedures, you should also read the following which are relevant to data protection:

   - The School's Privacy Notices for staff, pupils, parents and alumni; and
   - The School's policy on Staff Acceptable Use of IT (within the Staff Conduct Policy)

3. This policy applies to all staff (which includes Governors, agency staff, contractors, work experience students and volunteers) when handling Personal Data. For more information on what Personal Data is, please see the School's Data Protection Policy and Compliance Procedures.

4. Any questions or concerns about your obligations under this policy should be referred to the Operations and Compliance Director. Questions and concerns about technical support or for assistance with using the School IT systems should be referred to the IT Department.

Be aware

5. Information security breaches can happen in a number of different ways. Examples of breaches which have been reported in the news include:
   - an unencrypted laptop stolen after being left on a train;
   - Personal Data taken after website was hacked;
   - sending a confidential email to the wrong recipient;
   - leaving confidential documents containing Personal Data on a doorstep; and
   - using carbon copy (cc) rather than blind carbon copy (bcc) to send emails to multiple recipients.

6. These should give you a good idea of the sorts of things which can go wrong, but please have a think about what problems might arise in your team or department and what you can do to manage the risks. Speak to your manager if you have any ideas or suggestions about improving practices in your team. One option is to have team specific checklists to help ensure data protection compliance.

7. You must immediately tell the Operations and Compliance Director or the IT Network Manager if you become aware of anything which might mean that there has been a security breach. You must provide all of the information you have. If it is outside of school hours then please use these

emergency contact numbers (07590 037742 for Operations and Compliance Director or 07391 682164 for IT duty telephone). All of the following are examples of a security breach:

- you accidently send an email to the wrong recipient;
- you cannot find some papers which contain Personal Data; or
- any device (such as a laptop or a smartphone) used to access or store Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

8. In certain situations the School must report an information security breach to the Information Commissioner's Office (the data protection regulator) and let those whose information has been compromised know within strict timescales. This is another reason why it is vital that you report breaches immediately.

Thinking about privacy on a day to day basis

9. We should be thinking about data protection and privacy whenever we are handling Personal Data. If you have any suggestions for how the School could protect individuals' privacy more robustly please speak to the Operations and Compliance Director.

10. From May 2018, the School is required to carry out an assessment of the privacy implications of using Personal Data in certain ways. For example, when we introduce new technology, where the processing results in a risk to individuals' privacy or where Personal Data is used on a large scale, such as CCTV.

11. These assessments should help the School to identity the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required please let the Operations and Compliance Director know.

Critical School Personal Data

12. Data protection is about protecting information about individuals. Even something as simple as a person's name or their hobbies count as their Personal Data. However, some Personal Data is so sensitive that we need to be extra careful. This is called Critical School Personal Data in this policy and in the Data Protection Policy and Compliance Procedures for Staff.

    Critical School Personal Data is:

    - information concerning child protection matters;
    - information about serious or confidential medical conditions and information about special educational needs;
    - information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
    - financial information (for example about parents and staff);
    - information about an individual's racial or ethnic origin; and
        - political opinions;
        - religious beliefs or other beliefs of a similar nature;
        - trade union membership;
        - physical or mental health or condition;
        - genetic information;
        - sexual life;
    - information relating to actual or alleged criminal activity; and
    - biometric information (e.g. a pupil's fingerprints).

    <u>Staff need to be extra careful when handling Critical School Personal Data.</u> Specific advice is available from the IT Network Manager and Compliance Department.

Minimising the amount of Personal Data that we hold

13. Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe. If you would like guidance on when to delete certain types of information please speak to the Operations and Compliance Director.

Using computers and IT

14. A lot of data protection breaches happen as a result of basic mistakes being made when using the School's IT system. Here are some tips on how to avoid common problems:

    Lock computer screens: Your computer screen should be locked when it is not in use, even if you are only away from the computer for a short period of time. To lock your computer screen press the "Windows" key followed by the "L" key. If you are not sure how to do this then speak to the IT department.

    Be familiar with the School's IT: You should also make sure that you familiarise yourself with any software or hardware that you use. In particular, please make sure that you understand what the software is supposed to be used for and any risks. For example:

    - when using SharePoint, Microsoft Teams, or any "virtual classroom" which allows you to upload lesson plans and mock exam papers for pupils then you need to be careful that you do not accidently upload anything more confidential;
    - make sure that you know how to properly use any security features contained in School software; and
    - you need to be extra careful where you store information containing Critical School Personal Data. If in doubt, speak to the Operations and Compliance Director.

Hardware and software not provided by the School

15. Staff must not use, download or install any software, app, programme, or service into the School IT system without permission from the IT Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the School IT systems without permission. Private cloud storage: You must not use private cloud storage or file sharing accounts to store or share School documents containing Critical School Personal Data.

Portable media devices

16. The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed for any material containing personal data unless those devices have been given to you by the School and you have received training on how to use those devices securely.

Disposal of School IT equipment

17. School IT equipment (this includes laptops, printers, phones, and DVD drives) must always be returned to the IT Department even if you think that it is broken and will no longer work, so that secure disposal can be arranged.

Passwords

18. Passwords should be strong, difficult to guess, not disclosed to anyone else and not written down. For advice on what makes a strong password please speak to the IT Network Manager.

Emails (and faxes)

19. When sending emails or faxes you must take care to make sure that the recipients are correct.

20. Emails to multiple recipients: A blind carbon copy (bcc) function must be used when sending emails to multiple external email recipients so that names and email address are not visible to other recipients.

21. If the email or fax contains Critical School Personal Data then you should ask another member of staff to double check that you have entered the email address / fax number correctly before pressing send. If a fax contains Critical School Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

Encryption

22. Remember to encrypt internal and external emails which contain Critical School Personal Data. For example, encryption should be used when sending details of a safeguarding incident to social services. To use encryption, you need to contact the IT Network Manager to request access to appropriate software. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this should be provided via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password. Passwords for encrypted documents must not be sent in the same message as the attachment.

Private email addresses

23. You must not use a private email address for School related work. You must only use your @stjohns.surrey.sch.uk address. Please note that this rule applies to Governors as well.

Paper files

24. Keep under lock and key: Staff must ensure that papers which contain Personal Data are kept under lock and key in a secure location and that they are never left unattended on desks (unless the room is secure). Any keys must be kept safe.

25. If the papers contain Critical School Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information must not be stored in any other location, for example, safeguarding and child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (DSL) room. These are special cabinets used by the School which are fire proof and are kept in a secure location. They are also too heavy to move to minimise the risk of theft. Please speak to the Operations and Compliance Director if you are unsure as to whether your papers contain Critical School Personal Data and where they should be securely stored.

26. Disposal: Paper records containing Personal Data should be disposed of securely using the School's confidential waste disposal service. Personal Data should never be placed in the general waste.

27. Printing: When printing documents, make sure that you collect everything from the printer straight away, otherwise there is a risk that confidential information might be read or picked up by someone else. If you see anything left by the printer which contains Personal Data then you must hand it in to the Operations and Compliance Director.

28. Put papers away: You should always keep a tidy desk and put papers away when they are no longer needed. Staff are provided with their own personal secure cabinet(s) in which to store papers. However, these personal cabinets should not be used to store documents containing Critical School Personal Data.

29. Post: You also need to be extra careful when sending items in the post. Confidential materials should not be sent using standard post. If you need to send something in the post that is confidential, consider asking the IT Department to put in on an encrypted memory stick, or arrange for it to be sent by courier.

Working off-site

30. Staff might need to take Personal Data off the School site for various reasons, for example because they are working from home or supervising a School trip. This does not breach data protection law if the appropriate safeguards are in place to protect Personal Data.

31. For School trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You should seek advice from the Educational Visits Coordinator (Sally Hunt) or the Operations and Compliance Director about how to travel with Critical School Personal Data and keep it secure.

32. Not all staff are allowed to work from home but if you are then check with the Operations and Compliance Director or IT Network Manager about what additional information security arrangements should be in place. In most cases, if you have a School laptop information will be kept securely. If you are using a personal device at home, this is permitted for School-based applications, as long as you do not download data to the personal device. (See **Using personal devices for School work** below).

33. Take the minimum with you: When working away from the School you must only take the minimum amount of information with you. For example, a teacher organising a field trip might need to take with her information about pupil medical conditions (for example allergies and medication). If only eight out of a class of twenty pupils are attending the trip, then the teacher should only take the information about the eight pupils.

Working on the move

34. You must not work on documents containing Personal Data whilst travelling if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see what you are doing). For example, if working on a laptop on a train, you should ensure that no one else can see the laptop screen and you should not leave any device unattended where there is a risk that it might be taken.

35. Paper records: If you need to take hard copy (i.e. paper) records that contain Personal Data with you then you should make sure that they are kept secure. For example:

    - documents should be kept in a bag that can be locked. They should also be kept somewhere secure in addition to being kept in a locked bag if left unattended (e.g. overnight);
    - if travelling by train you must keep the documents with you at all times and they should not be stored in luggage racks;
    - if travelling by car, you must keep the documents out of plain sight. Please be aware that possessions left on car seats are vulnerable to theft when your car is stopped e.g. at traffic lights;
    - if you have a choice between leaving documents in a vehicle and taking them with you (e.g. to a meeting) then you should usually take them with you and keep them on your person in a locked bag. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked bag in the vehicle out of plain sight. The risks of this situation should be reduced by only having the minimum amount of Personal Data with you.

36. Public Wi-Fi: You must not use public Wi-Fi to connect to the internet. For example, if you are working in a cafe then you will either need to work offline or use 3G / 4G.

37. Critical School Personal Data should not be taken off the site in paper format.

Using personal devices for School work

38. You may only use your personal device (such as a smartphone, tablet or laptop) for School work if you have been given permission by the IT Network Manager, agreed to the terms and conditions and completed installation of the Smoothwall certificate.

39. Appropriate security measures should always be taken, such as using firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

40. You must not send documents that contain School personal data to your personal email accounts, or save them to your personal device.

41. Friends and family: You must take steps to ensure that others who use your device (for example, friends and family) cannot access anything School related on your device. For example, you should not share the login details with others and you should log out of your account once you have finished working by restarting your device. You must also make sure that your devices are not configured in a way that would allow someone else access to School related documents and information – if you are unsure about this then please speak to the IT Network Manager.

42. If you stop using your device for School work, for example:
    - if you decide that you do not wish to use your device for School work; or
    - if the School withdraws permission for you to use your device; or
    - if you are about to leave the School

    then, all School documents (including School emails), and any software applications provided by the School, for School purposes, will be removed from the device. If this cannot be achieved remotely, you must submit the device to the IT Department for wiping and software removal. You must provide all necessary co-operation and assistance to the IT Department in relation to this process.

Breach of this policy

43. Any breach of this policy will be taken seriously and may result in disciplinary action.

44. A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

45. This policy does not form part of any employee's contract of employment.

46. We reserve the right to change this policy at any time. Where appropriate, we will notify staff of those changes by mail or email.