St John's Catholic Primary School

BATH

Email: stjohnsbath_pri@bathnes.gov.uk
Website: www.stjohnscatholicprimary.org.uk

Head Teacher: Mrs A Bennett

Information Security Policy 2018/21

I am unique,
In the eyes of God.
All seeing, all knowing, all loving,
He embraces our family,
Parish, parent, child,
All one with you.
I am of the world,
With the seeds of excellence within me,
Encouraged to grow and flourish,
To a spiritual fulfilment.
I am unique,
And with you beside me,
All is possible

1 Introduction

1.1 Information security is about what you and the School should be doing to make sure that School 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.

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

1.2.1 privacy notice for staff; and

1.2.2 IT acceptable use policy.

[note: please put in any other policies which should be listed above.]

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

1.4 Any questions or concerns about your obligations under this policy should be referred to The Headteacher. Questions and concerns about technical support or for assistance with using the School IT systems should be referred to the IT Subject Leader.

2 Be aware

2.1 Information security breaches can happen in a number of different ways: Examples of breaches which have been reported in the news include:

2.1.1 unencrypted laptop stolen after being left on a train;

2.1.2 Personal Data taken after website was hacked;

2.1.3 sending a confidential email to the wrong recipient;

2.1.4 leaving confidential documents containing Personal Data on a doorstep; and

2.1.5 using carbon copy rather than blind carbon copy to send emails to multiple recipients.

2.2 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 and the Data Protection Officer if you have any ideas or suggestions about improving practices in your team.

2.3 You should immediately report all security incidents, breaches and weaknesses to the Data Protection Officer. This includes anything which you become aware of even if you are not directly involved (for example, if you know that document storage rooms are sometimes left unlocked at weekends).

2.4 You must immediately tell the Data Protection Officer and the IT Subject Leader if you become aware of anything which might mean that there has been a security breach. For example, if:

2.4.1 you accidently send an email to the wrong recipient;

2.4.2 you cannot find some papers which contain School Personal Data; or

2.4.3 any device (such as a laptop or a smartphone) used to access or store School Personal Data has been lost or stolen or you suspect that the security of a device has been compromised.

3 Critical School Personal Data

3.1 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. Critical School Personal Data is:

3.1.1 information concerning child protection matters;

3.1.2 information about serious or confidential medical conditions and information about special educational needs;

3.1.3 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);

3.1.4 financial information (for example about parents and staff); and

3.1.5 information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life and information relating to actual or alleged criminal activity.

3.2 Staff need to be extra careful when handling Critical School Personal Data.

4 Using computers and IT

4.1 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.

4.2 **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 following by the “L” key. If you are not sure how to do this then speak to IT.

4.3 **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:

4.3.1 if you use a "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;

4.3.2 make sure that you know how to properly use any security features contained in School software. For example, some software will allow you to redact documents (i.e. "black out" text so that it cannot be read by the recipient). Make sure that you can use this software correctly so that the recipient of the document cannot "undo" the redactions; and

4.3.3 you need to be extra careful where you store information containing Critical School Personal Data, if in doubt, speak to the Data Protection Officer. For example,

safeguarding information should not ordinarily be saved using alumni database software.

4.4 Specific information on the different programmes that the School uses can be found on the staff shared drive

4.5 **Hardware and software not provided by the School:** Staff must not use, download or install any software, app, programme, or service without permission from the IT Subject Leader. 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 first signing permission.

4.6 **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share School documents.

4.7 **Portable media devices.** The use of portable media devices (such as USB drives, portable harddrives, DVDs) is not allowed unless those devices have been given to you by the School and you have received training on how to use those devices securely.

4.8 **Disposal of School IT equipment:** School IT equipment (and this includes laptops, printers, phones, and DVDs etc) must always be returned to the IT Department even if you think that it is broken and will no longer work.

5 Passwords

5.1 Passwords should be a mix of uppercase and lowercase, numbers and special characters (i.e. #, &, !), should be at least eight characters in length and should not be disclosed to anyone else.

5.2 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know.

5.3 Passwords should be changed regularly (for example every month) and your updated password should not be similar to the previous one (for example do not change your password by just adding a number each time, e.g. orchard1, orchard2, orchard3 etc).

5.4 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

6 Emails (and faxes)

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

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

6.3 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.

6.4 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.

6.5 **Encryption:** Remember to encrypt 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 then you need to speak to IT. 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 them with the password.

6.6 **Private email addresses:** You must not use a private email address for School related work. You must only use your school email address.

7 Paper files

7.1 **Keep under lock and key:** Staff must ensure that papers which contain School 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.

7.2 If the papers contain **Critical School Personal Data** then they must be kept in secure cabinets when not being used as set out in the table below. Information must not be stored in any other location. For example, child protection information should only be stored in the cabinet in the Headteacher's Office and the SENCo Office.

Cabinet	**Access**
Child protection - located in the Headteacher's Office and the SENCo office	The Headteacher, the two deputy headteachers and the SENCo know where the key is for this Cabinet.
[Financial information - located in the School Office	The Headteacher, the Office Manager and the School Bursar know where the key is for this.
Individual Pupil Files located in the School Office	The Headteacher, and Office Manager know where the key is for this.
Individual Staff Files located in the School Office	The Headteacher, and Office Manager know where the key is for this

7.3 **Disposal:** Paper records containing School Personal Data should be disposed of securely by placing them in confidential waste bins which are located around the school. School Personal Data should never be placed in the general waste.

7.4 **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 School Personal Data then you must hand it in to the person that printed it or the Headteacher. The school is investigating a "follow me" printing which means that you cannot print something out unless standing by the printer, and entering your access code.

7.5 **Put papers away:** You should always keep a tidy desk and put papers away when they are no longer needed. Staff are provided with a cupboard in each classroom which is lockable for staff to store documents, such as IEPs, Assessment Data etc

7.6 **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 your IT team to put in on an encrypted memory stick or arrange for it to be sent by courier.

8 Working off site (e.g., School trips and homeworking)

8.1 Staff might need to take School 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 School Personal Data.

8.2 For School trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it.

8.3 If you are allowed to work from home then check with the Data Protection Officer what additional arrangements are in place. This might involve installing software on your home computer or smartphone, please see section 9 below.

8.4 Not all staff are allowed to work from home. If in doubt, speak to the Data Protection Officer.

8.5 **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 etc). 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.

8.6 **Working on the move:** You must not work on documents containing School 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.

8.7 **Paper records:** If you need to take hard copy (i.e. paper) records with you then you should make sure that they are kept secure. For example, 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 if left unattended. Documents should be kept in a locked case. They should also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight).

8.8 **Public wifi:** You must not use public wifi to connect to the internet. For example, if you are working in a cafe then you will either need to work off-line or use 3G/4G.

8.9 **Using School laptops, phones, cameras and other devices:** If you need to book out a School device then the school office will sign out the device.

9 Using personal devices for School work

9.1 You may only use your personal device (such as your laptop or smartphone) for School work if you have been given permission by the Data Protection Officer.

9.2 Even if you have been given permission to do so, then before using your own device for School work you must speak to your IT team so that they can configure your device.

9.3 **Using your own PC or Laptop:** If you use your laptop or PC for School work then you must use the remote access software provided by the School known as [• name of software]. Using [• name of software] means that School Personal Data is accessed through the School's own network which is far more secure and significantly reduces the risk of a security breach.

9.4 **Using your own smartphone or handheld:** Before you use your own smartphone or handheld for School work you must install the device management software provided by the School which will help keep School Personal Data secure and separate from private files.

9.5 This software is called [• name of device management software]. The software has remote wipe functionality which can be invoked should the device be lost or stolen. The School reserves the right to monitor, review and erase, without further notice, all content on the device that has been created for the School or on the School's behalf or which contains School Personal Data. Although we do not intend to wipe other data that is private in nature (such as private photographs or private files or emails), it may not be possible to distinguish all such information from School Personal Data in all circumstances. You should therefore regularly back up any private data contained on the device or keep private material separate via a partition that would not be remotely wiped in these circumstances.

9.6 You must not do anything which could prevent any software installed on your computer or device by the School from working properly. For example, you must not try and uninstall the software, or save School related documents to an area of your device not protected, without permission from the IT Department first.

9.7 **Appropriate security measures** should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date.

9.8 **Sending or saving documents to your computer:** Documents containing School Personal Data should not normally be sent to or saved to personal devices, unless you have been given permission by the IT Department. This is because anything you save to your computer will not be protected by the School's security systems. Furthermore, it is often very difficult to delete something which has been saved to a computer. For example, if you saved a School document to your laptop because you wanted to work on it over the weekend, then the document would still be on your computer hard drive even if you deleted it and emptied the recycle bin.

9.9 **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 Subject Leader.

9.10 **When you stop using your device for School work**: If you stop using your device for School work, for example:

9.10.1 if you decide that you do not wish to use your device for School work; or

9.10.2 if the School withdraws permission for you to use your device; or

9.10.3 if you are about to leave then School

then, all School documents (including School emails), and any software applications provided by us for School purposes, will be removed from the device.

If this cannot be achieved remotely, you must submit the device to the IT Lead for wiping and software removal. You must provide all necessary co-operation and assistance to the the IT department in relation to this process.

10 Breach of this policy

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

10.2 A member of staff who deliberately or recklessly discloses School 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.

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

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

I confirm that I have read and understood the contents of this policy:

I will sign the school GDPR Form, confirming that I have read this policy and all others relating to GDPR.

Signed: _____

Chair of Governors:_____

Reviewed: 3rd July 2018

Due Review: July 2021

Appendix 1 School Applications

TO BE COMPLETED BY SUBJECT LEADERS AND OFFICE TEAM.

Application	What it can be used for	Specific security arrangements	Any other notes / comments
[Example:123 Alumni Database]	[Storing alumni information only.]	[Only the following staff have permission to access the database: [please complete] Different staff have different permission levels, if you need additional permissions, please speak to the Data Protection Officer.]	[Although the School works closely with the alumni association, you must not allow them access to the database without permission from the [Data Protection Officer].]
SIMS			