Information Security Policy

Information Security Policy 2019

This policy has been drafted to make staff aware of their obligations under both the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) , which replaced the Data Protection Act 1998 from 25 May 2018. Although the DPA 2018 and the GDPR now apply, there remains some uncertainty around their application, particularly as the ICO continue to publish new guidance. As such the document will likely need to be updated in due course.

Review Date: Sept 2020

1 Introduction

1.1 Information security is about what you and Inspired Learning Group (**ILG**) 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.

1.2 ILG operates St Christopher's School (the **School**). ILG is ultimately responsible for how you handle personal information. In this policy, we use the term "ILG" to mean both the School and ILG.

1.3 This policy should be read alongside these policies which are relevant to data protection:

1.3.1 ILG's privacy notices for staff, pupils and parents; and

1.3.2 IT acceptable use policy for staff.

1.4 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 ILG's data protection policy.

1.5 Any questions or concerns about your obligations under this policy should be referred to the Headteacher, who will liaise with the the Head of Regulations and Business Development.

From this point on, reference to the Head of Regulations and Business Development will be interchangeable with the Headteacher, who will be tasked with forwarding questions or concerns. Questions and concerns about technical support or for assistance with using the ILG IT systems should be referred to RIKA technologies who control ILG IT systems.

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 an 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; and

2.1.4 leaving confidential documents containing Personal Data on a doorstep.

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 Head of Regulations and Business Development 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.

2.3 You should immediately report all security incidents, breaches and weaknesses to the Head or the Head of Regulations and Business Development]. 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 Head or the the Head of Regulations and Business Development] and the IT Department if you become aware of anything which might mean that there has been a data protection or security breach. This could be anything which puts Personal Data

at risk, for example, if Personal Data has been or is at risk of being destroyed, altered, disclosed or accessed without authorisation, lost or stolen. You must provide your manager or the Head of Regulations and Business Development with all of the information you have. If you cannot get hold of your manager or the Head of Regulations and Business Development or it is outside of school hours then please use the Headteacher's emergency number or the emergency contact number on the staff contact tree. All of the following are examples of a security breach:

2.4.1 you accidently send an email to the wrong recipient;

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

2.4.3 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.

2.5 In certain situations ILG 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.

3 Thinking about privacy on a day to day basis

3.1 We should be thinking about data protection and privacy whenever we are handling Personal Data. If you have any suggestions for how ILG could improve its data protection / information security practices or protect individual's privacy more robustly please speak to the Head of Regulations and Business Development.

3.2 In some situations, ILG 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 particular risk to an individual's privacy.

3.3 These assessments should help ILG to identify the measures needed to prevent information security breaches from taking place. If you think that such an assessment is required please let the Head of Regulations and Business Development know.

4 Critical Personal Data

4.1 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 Personal Data** in this policy and in the data protection policy. Critical Personal Data is:

4.1.1 information concerning child protection matters;

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

4.1.3 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);

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

4.1.5 information about an individual's racial or ethnic origin; and

4.1.6 political opinions;

4.1.7 religious beliefs or other beliefs of a similar nature;

4.1.8 trade union membership;

4.1.9 physical or mental health or condition;

4.1.10 genetic information;

4.1.11 sexual life or sexual orientation;

4.1.12 information relating to actual or alleged criminal activity; and

4.1.13 biometric information (e.g. fingerprints used for controlling access to a building).

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

5 Minimising the amount of Personal Data that we hold

5.1 Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe. You should never delete personal data unless you are sure you are allowed to do so. If you would like guidance on when to delete certain types of information please speak to the Head of Regulations and Business Development.

6 Using computers and IT

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

6.2 **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 followed by the "L" key. If you are not sure how to do this then speak to IT. ILG's computers are configured to automatically lock if not used for five minutes.

6.3 **Be familiar with ILG'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:

6.3.1 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;

6.3.2 make sure that you know how to properly use any security features contained in ILG 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

6.3.3 you need to be extra careful where you store information containing Critical Personal Data. For example, safeguarding information should not be saved on a shared computer drive accessible to all staff. If in doubt, speak to the Head of Regulations and Business Development.

6.4 **Hardware and software not provided by ILG:** Staff must not use, download or install any software, app, programme, or service 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 ILG IT systems without permission.

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

6.6 **Portable media devices:** The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices have been given to you by ILG and you have received training on how to use those devices securely. The IT Department will protect any portable media device given to you with encryption.

6.7 **ILG IT equipment:** If you are given ILG IT equipment to use (this includes laptops, printers, phones, and DVDs) you must make sure that this is recorded on ILG's IT equipment asset register]. ILG IT equipment must always be returned to the IT Department even if you think that it is broken and will no longer work and the asset register updated accordingly.

6.8 **Where to store electronic documents and information:** You must ensure that you only save or store electronic information and documents in the correct location on ILG's systems as follows:

6.8.1 [Set of where different types of information should be stored, eg, in ILG's IMS, cloud based services, or in a specific network location. If more convenient, link to where this information can be found on ILG's network rather than include in the policy.]

7 Passwords

7.1 Passwords should be long and difficult to guess, for example, you could use a song lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it's difficult to remember without writing it down. Your password should not be disclosed to anyone else.

7.2 You should not use a password which other people might guess or know, or be able to find out, such as your address or your birthday.

7.3 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any school account.

7.4 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.

8 Emails (and faxes)

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

8.2 **Emails to multiple recipients:** [• Describe protocol used to ensure emails to multiple recipients are sent securely e.g. special software / information management systems / protocol on who can send out those emails].

8.3 If the email or fax contains Critical 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 Personal Data then you must make sure that the intended recipient is standing by the fax machine to receive the fax.

8.4 **Encryption:** Remember to encrypt internal and external emails which contain Critical Personal Data. For example, WORD documents can be attached to email and encrypted with a password which can then be forwarded separately to the recipient.

8.5 **Private email addresses:** You must not use a private email address for ILG related work. You must only use your school address. Please note that this rule applies to Governors as well.

9 Paper files

9.1 **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.

9.2 If the papers contain Critical Personal Data then they must be kept in secure cabinets identified for the specified purpose as set out in the table below. Information held in paper form must not be stored in any other location, for example, child protection information should only be stored in the cabinet in the Designated Safeguarding Lead's (**DSL**) room]. These are special cabinets used by ILG and are kept in a secure location. They are also too heavy to move to minimise the risk of theft. The cabinets are located around the site as follows.

Cabinet	**Access**
Child protection - located in the DSL's office	Headteacher and DSL
Financial information - located in the HR Director's office	Headteacher
Health information and Single Central Register Information etc	Headteacher

9.3 **Disposal:** Paper records containing Personal Data should be disposed of securely shredding the material and disposing the paper waste in recycling. Personal Data should never be placed in the general waste.

9.4 **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 Personal Data then you must hand it in to the Head of Regulations and Business Development

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

containing Critical Personal Data. Please see paragraph 9.2 above for details of where Critical Personal Data should be kept.

9.6 **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.

10 Working off site (e.g. school trips and homeworking)

10.1 Staff might need to take Personal Data off the 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.

10.2 For school trips, the trip organiser should decide what information needs to be taken and who will be responsible for looking after it. You must make sure that Personal Data taken off site is returned to ILG or the school.

10.3 If you are allowed to work from home then check with the Head of Regulations and Business Development what additional arrangements are in place. This might involve working with a specially encrypted memory stick or installing software on your home computer or smartphone: please see section 11 below.

10.4 Not all staff are allowed to work from home. If in doubt, speak to the Head of Regulations and Business Development.

10.5 **Take the minimum with you:** When working away from your 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.

10.6 **Working on the move:** 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.

10.7 **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:

10.7.1 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);

10.7.2 if travelling by train you must keep the documents with you at all times and they should not be stored in luggage racks;

10.7.3 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;

10.7.4 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 case. However, there may be specific circumstances when you consider that it would be safer to leave them in a locked case 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 (please see paragraph 10.5 above).

10.8 **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.]

10.9 **Using ILG laptops, phones, cameras and other devices:** If you need to book out an ILG device then save all data on a specially encrypted memeory stick which remains the property of ILG.

10.10 Critical Personal Data should not be taken off the site in paper format save for specified situations where this is absolutely necessary, for example, where necessary for school trips (see 10.5 above).

11 Using personal devices for school work

11.1 You may only use your personal device (such as your laptop or smartphone) for school work if you have been given permission by the Head of Regulations and Business Development. Please also see paragraph 6.8 above.

11.2 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.

11.3 **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.

11.4 **Default passwords**: If you use a personal device for school work which came with a default password then this password should be changed immediately. Please see section 7 above for guidance on choosing a strong password.

11.5 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) should not 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, tablet or mobile phone will not be protected by ILG'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.

11.6 **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 Department.

11.7 **When you stop using your device for school work:** If you stop using your device for school work, for example:

11.7.1 if you decide that you do not wish to use your device for school work; or

11.7.2 if the school withdraws permission for you to use your device; or

11.7.3 if you are about to leave ILG

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 Department for wiping and software removal. You must provide all necessary co-operation and assistance to the the IT department in relation to this process.

12 Breach of this policy

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

12.2 A member of staff who deliberately or recklessly obtains or discloses Personal Data held by ILG without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal. Further information on this and on other offences can be found in ILG's data protection policy.

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

12.4 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:

Name	.....
Signature	.....
Date	_____Date/____ month/_____ year

Appendix A: Protocols and Guidance for the use of Mobile Phones in School

Personal mobile phones and mobile devices

Responsibility

- Mobile phones and personally-owned mobile devices brought into school are entirely at the staff member, pupil's & parents' or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- The recording, taking and sharing of images, video and audio on any mobile phone is prohibited; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to

scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- Mobile phones and personally-owned devices approved for use by the Head in exceptional circumstances are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.

Staff

- All staff (EYFS and School) mobile phones must be secured in the locked cabinets provided
- Staff members may use their phones during school break times in certain areas.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with pupils, parents or carers is required. Staff will also be issued with a school phone whilst on educational off-site visits. Alternatively, staff may have permission from the Headteacher or the Educational Visits Co-ordinator to bring their own mobile phones on trips – to be used strictly for communication with the school or for emergency situations.
- Approved by Head Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Visitors

All visitors are requested to keep their phones on silent.

Parents and Pupils

- Where parents or pupils need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Pupils' use of personal devices

- The School strongly advises that pupil mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into tests of examinations in or out of **St Christopher's**. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- No pupils should bring his or her mobile phone or personally-owned device into school. Any device brought into school will be confiscated.
-

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign that they have read the school's full Information Security Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;

- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include Directors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.