Information Security Policy

Inspired Learning Group

August 2024

Contents

1 Introduction

1.1 Information security is about what you and ILG need to do to help make sure that **Personal Data** is kept safe. This is the most important area of data protection to get right. Most data protection fines have come about because of information security breaches.

1.2 All staff are obliged to comply with ILG's policies, processes and guidance related to the handling and security of Personal Data. Any breach may result in disciplinary action.

1.3 Data Protection is the responsibility of everyone at ILG, and it is important that you read and understand the relevant policies so that you know what you should do day-to-day, but also what to do when something goes wrong.

1.4 Any questions or concerns about your obligations under this policy must be referred to the data protection lead within your setting or Head Office. Questions or concerns about technical support or for assistance with using the ILG IT systems must be referred to the IT department.

1.5 In the event of a significant security incident or data breach and you are unable to contact your setting's data protection lead/senior leader, or it is outside of normal working hours, you can contact the Chief Privacy Officer on 07789 882597.

2 Application

2.1 This policy applies to all staff working at ILG (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, contractors, peripatetic teachers, agency staff, work experience / placement students, apprentices and volunteers.

2.2 This policy is for internal use only, not for publication on any of our websites. This policy can be found on Sharepoint under ILG Head Office External - Documents\GDPR\Policies. It is also available on request from the setting or Head Office.

2.3 Employees only: This policy does not form part of a contract of employment and may be amended by ILG at any time.

3 Be aware

3.1 Information security breaches can happen in a number of different ways. Examples include:

3.1.1 opening a suspicious attachment on an email;

3.1.2 not being able to access the only copy of a document because the password has been forgotten;

3.1.3 an unencrypted laptop stolen after being left on a train;

3.1.4 Personal Data held to ransom following a website hack;

3.1.5 sending a confidential email to the wrong recipient; and

3.1.6 leaving confidential documents containing Personal Data on a doorstep.

3.2 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 line manager or the data protection lead within your setting or Head Office if you have any ideas or suggestions about improving practices in your team.

3.3 You must immediately inform the data protection lead within your setting or Head Office if you become aware of anything which might mean that there has been a security incident or data breach or if you become aware of a practice that weakens ILG's defences in relation to the protection of Personal Data. 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. Another example might be where you become aware that a particular department has developed a habit of leaving confidential documents in unlocked classrooms. You must provide the data protection lead within your setting or Head with all of the information you have. You must report even if you are not certain that something has gone wrong. For example, if you accidentally send an email to the wrong recipient, or you cannot find some papers which contain Personal Data. You must report this even if there is no evidence that they have been accessed or stolen.

3.4 In certain situations, ILG must report certain data breaches to the Information Commissioner's Office (the data protection regulator) within 72 hours, and let those whose information has been compromised know within strict timescales as well. This is another reason why it is vital that you report breaches immediately.

3.5 You should report even if you are not directly involved.

4 Thinking about privacy on a day to day basis

4.1 You should be thinking about data protection and privacy whenever you are handling Personal Data. Personal Data is virtually anything recorded about someone, even something as simple as a person's address or hobbies. 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 data protection lead within your setting or Head Office.

4.2 In some situations, ILG and the settings are required to carry out an assessment of the privacy implications of using Personal Data in certain ways. These assessments are known as data protection impact assessments. For example, when new technology is introduced which represents a particular risk to an individual's privacy.

4.3 These assessments should help ILG and the settings to identify the measures needed to prevent information security breaches from taking place

5 Critical or Sensitive Personal Data

5.1 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 or Sensitive Personal Data** in this policy and in the data protection policy.

5.2 This type of Personal Data is information which concerns:

5.2.1 safeguarding or child protection matters;

5.2.2 serious or confidential medical conditions;

5.2.3 special educational needs;

5.2.4 financial information including parent and staff bank details;

5.2.5 an individual's racial or ethnic origin;

5.2.6 political opinions;

5.2.7 religious beliefs or other beliefs of a similar nature;

5.2.8 trade union membership;

5.2.9 someone's physical or mental health or condition;

5.2.10 sex life including sexual orientation;

5.2.11 actual or alleged criminal activity;

5.2.12 allegations made against an individual (whether or not the allegations amount to a criminal offence and whether or not the allegations have been proved);

5.2.13 biometrics (for example if fingerprint scanners are used for allowing access to buildings); and

5.2.14 genetic information.

5.3 Staff need to be extra careful when handling Critical or Sensitive Personal Data.

6 Minimising the amount of Personal Data that we hold

6.1 Restricting the amount of Personal Data we hold to that which is needed helps keep personal data safe but you must 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 data protection lead within your setting or Head Office.

7 Using computers and IT

7.1 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:

7.2 **Lock computer screens:** Your computer screen must 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. You can also configure your computer settings to automatically lock if not used for a certain period of time.

7.3 **Be familiar with ILG's IT:** You must 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:

7.3.1 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;

7.3.2 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

7.3.3 you need to be extra careful where you store information containing Critical or Sensitive Personal Data, especially safeguarding information. If in doubt, speak to the data protection lead within your setting or Head Office.

7.4 **Hardware and software not provided by ILG:** Staff must not use, download or install any software, app, programme, or service without permission from the Head/Nursery Manager, IT Department or the Head of Department. Staff must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the ILG IT systems without permission.

7.5 **Private cloud storage:** You must not use private cloud storage or file sharing accounts to store or share workl documents. You must only use cloud storage provided by ILG.

7.6 **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 provided or sanctioned by ILG or the setting, they do not contain any Personal Data, and you know how to use those devices securely. Portable media devices must be protected with suitable encryption. Be aware that anything not provided or sanctions by ILG or the setting may be harmful even if it looks innocuous.

8 **IT equipment:** If you are given IT equipment to use (this includes laptops, printers, phones, and DVDs), you must make sure that this is recorded on ILG's equipment asset register. IT equipment must always be returned even if you think that it is broken and will no longer work and the asset register updated accordingly. Each setting and Head Office is responsible for ensuring that any electronic devices are wiped securely before they are disposed of or recycled. This can be done remotely if required.

8.1 **Where to store electronic documents and information:** You must ensure that you only save or store electronic information and documents in the correct location, as advised by ILG or the setting.

9 Passwords

9.1 Passwords are usually provided by the IT Department, but can be changed. Passwords must be as long as possible and difficult to guess. Do not use single dictionary words. Instead use a passphrase which you create by stringing some words and / or numbers together. Make sure this phrase is memorable but don't choose words or numbers that are linked to you like the names of your family members. Do not choose a password which is so complex that it's difficult to remember without writing it down.

9.2 You must not use a company password which you use for another private account. For example, you must not use your password for your private email address or online shopping account for any school or work account. This is because if your personal account is compromised this presents a risk of access to ILG's systems as well.

9.3 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 must not be written down.

9.4 Sometimes a computer or web browser will allow you to save the password so that you do not need to type it in again next time. This can only be done if you are the sole user of a laptop. Be aware that pupils can also pose a risk to ILG, particularly those pupils who have a good understanding of IT. Many schools have had their computer systems compromised by pupils. If you have any suspicions please raise this.

10 Cyber security and related risks

10.1 Schools are frequently targeted by attackers looking to take advantage of vulnerabilities in school systems and processes. Sometimes, such attacks will look to exploit technical weaknesses whilst on other occasions, attacks will focus on the human element. For example, they might encourage someone to click on a link in an email by making the email appear as if it has come from a trusted source such as a colleague.

10.2 The following are examples of the types of things to look out for:

10.2.1 a request for information, especially financial information;

10.2.2 a request to click a link or open an attachment;

10.2.3 the sender telling you that it is urgent;

10.2.4 poor language or spelling;

10.2.5 a payment request from a supplier using an email address that is not their usual email address;

10.2.6 unusual sender details or an email address that doesn't look quite right. Often someone may try to pretend that they are emailing you from a School email address. For example, the email address after the @ symbol might contain the name of your school but the spelling is incorrect or the suffix at the end of the email might be different i.e. not .com or .co.uk.

10.3 Alternatively, an email may appear as if it's from someone who is providing technical support. For example, if might ask for your password or other credentials. Never share your password with anyone. IT will never ask for this.

10.4 If you find that you cannot access a particular programme, system or set of data, you must contact your IT team immediately. Whilst this could just be a technical fault, it could be evidence that someone has been able to gain access to ILG's systems.

10.5 Sometimes the attacker may be someone known to ILG, such as a parent or pupil. For example, following an acrimonious divorce a parent may set up an email address using the other parent's name in order to try to trick ILG into sending them information concerning the other parent.

10.6 If you are asked to provide personal data over the phone make sure that the request is genuine. For example, by calling the individual back using the number you have on the system. This must be done even if the person says that they are in a position of authority, such as the police.

10.7 Sometimes hackers create fake links to advertisements which are displayed on websites. When you click on the link or advert a malicious programme is downloaded.

10.8 You must also be on your guard if anyone asks you to change Personal Data held by ILG. Compromising the accuracy of Personal Data is also a breach, even if it is accidental.

10.9 If you fall victim to any form of scam or attack, you MUST report this immediately so that ILG can take the necessary steps to minimise the impact of the action, and report where necessary.

10.10 If you have any suspicions or concerns, or need to report a potential attack, immediately tell the data protection lead within your setting or Head Office, or the IT Department.

11 Email and telephone

11.1 You must take care to make sure that the recipients are correct. Getting an email address or telephone number wrong is one of the most common causes of a breach.

11.2 Double check email attachments before sending.

11.3 **Emails to multiple recipients:** Particular care must be taken when sending emails to multiple recipients. Check that they are as intended, and do not contain information which should not be shared with others. It is not always necessary to hide email addresses. For example, when sending a routine email to staff about a timetable change. However in some situations they must be hidden. For example, when sending a newsletter or general information to parents.

11.4 **Critical or Sensitive Personal Data:** If an email contains this type of Personal Data, you must seek prior approval from your line manager prior to sending. Ask another member of staff to double check that you have entered the email address correctly, and that the information is appropriately encrypted as explained below.

11.5 **Encryption:** Remember to encrypt internal and external emails which contain Critical School Personal Data. For example, encryption must be used when sending details of a safeguarding incident to social services, or information about a child's special educational needs to the local authority. If you need to give someone the "password" or "key" to unlock an encrypted email or document then this must be provided via a different means. For example, after emailing the encrypted documents you may wish to call the recipient with the password.

11.6 **Non-school email addresses:** You must not use a private email address for School related work. You must only use a school or ILG email address, which is usually set up when you start work. Please speak to the IT Department if this is not the case, and you require an email account to be set up for you.

12 Paper files

12.1 **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. If you take Personal Data with you to a meeting make sure that you collect all of your papers when you leave.

12.2 If the papers contain Critical or Sensitive Personal Data then they must be kept in secure, fire proof cabinets identified for a specified purpose. These cabinets are usually heavy, minimising the risk of theft. A secure safe is another location that can be used. Some examples are provided in the table below, which can be adapted and expanded according to the needs and structure of the setting or Head Office. However each setting and departmental managers within ILG are responsible for identifying and managing secure locations for their own paper files to be stored. For each cabinet, a procedure should be set out for access and who holds the key (there must be at least two people so it can always be accessed in an emergency).

Type of information	**Suggested locations of cabinets**
Safeguarding and child protection and records	Head or DSL office
Staff SCR and HR files	Head or HR lead/Bursar office (through schools and HO)
Printouts of SCR spreadsheet and Admission Register (historic 3 years)	Head or School Admin office
Financial information	HR lead/Bursar or Finance office (through schools and HO)
Pupil SEN files and EHCPs	Head or SENCO office

12.3 **Disposal:** Paper records containing Personal Data must be disposed of securely. This can be done via confidential waste bins if available, or by using an outside contractor, or by shredding. Personal Data must never be placed in the general waste.

12.4 **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 data protection lead within your setting or Head Office.

12.5 **Put papers away:** You must always keep a tidy desk and put papers away when they are no longer needed. Drawers are available in most desks, or on request if needed (state if lockable drawers are required).

12.6 **Displays:** Be aware of what Personal Data is on display when the classroom is being used for lessons. For example, would it be possible for pupils to read information that is on your desk while you are teaching?

12.7 **Post:** You also need to be extra careful when sending items in the post. Confidential materials, including anything which contains Critical or Sensitive Personal Data, must not be sent using standard post. If you need to send something in the post that is confidential, consider asking for an encrypted memory stick or arrange for it to be sent by courier.

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

13.1 Staff might need to take Personal Data off the School sites for various reasons, for example if 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.

13.2 For School trips, the trip organiser is responsible for deciding what information needs to be taken and who will look after it. You must make sure that Personal Data taken off site is returned to the School.

13.3 If your role enables you to work from home, check with the data protection lead within your setting or Head Office as to what additional arrangements need to be in place with regard to paper records and accessing information electronically. You must never email work containing personal data to your personal email address.

13.4 **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 them 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 must only take the information about the eight pupils.

13.5 **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 must ensure that no one else can see the laptop screen and you must not leave any device unattended where there is a risk that it might be taken.

13.6 **Return the documents:** Make sure that documents are returned to the School. For example, if you print off some information for a school trip, make sure the print out is returned to the School.

13.7 **Paper records:** If you need to take hard copy (i.e. paper) records off School site then you must make sure that they are kept secure. For example:

13.7.1 documents must be kept in a locked case. They must also be kept somewhere secure in addition to being kept in a locked case if left unattended (e.g. overnight);

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

13.7.3 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 or parked. Never leave any IT equipment or sensitive documents in a vehicle overnight;

13.7.4 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 13.4 above).

13.8 **Public Wi-Fi:** Be aware of the risks when using public Wi-Fi to connect to the internet. For example, if you are working in a cafe then you will need to consider working offline or using 4G.

13.9 **Using School laptops, iPads, phones, cameras and other devices:** If you need to book out a School device, follow the process in place at your setting.

13.10 Critical or Sensitive Personal Data must 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 as outlined above. Other than School trips, you must obtain authorisation from the data protection lead within your setting or Head Office.

13.11 **When you finish at ILG:** When you leave ILG (e.g. to start a new job or to retire) you must return any IT equipment and Personal Data (including documents containing persona data) to the data protection lead or HR function within your setting or Head Office, or to your line manager before the end of your last day (or earlier if requested). For example, if you have been given permission to keep papers at home you will need to make sure that these are returned.

14 Using personal devices for work

14.1 You may only use your personal devices (such as your laptop or phone) for work if you have been given permission by the Head/Nursery Manager or data protection lead within your setting or Head Office.

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

14.3 **Using your own laptop or PC:** If you use your own laptop or PC for work, you must use the remote access software provided by ILG. This means that Personal Data is accessed through ILG's own network, which is far more secure and significantly reduces the risk of a security breach.

14.4 **Using your own phone:** Before you use your own phone for work you must speak to the data protection lead within your setting or Head Office. Depending on your role and the use of your phone, they may ask you to install the device management software provided by ILG which will help keep Personal Data secure and separate from private files.

14.5 The software provided by ILG has remote wipe functionality which can be invoked should the device be lost or stolen. ILG reserves the right to monitor, review and erase, without further notice, all content on the device that has been created for ILG or on ILG's behalf or which contains 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 Personal Data in all circumstances. You must therefore regularly back up any private data contained on the device.

14.6 You must not do anything which could prevent any software installed on your computer or device by ILG from working properly. For example, you must not try and uninstall the software, or save work related documents to an area of your device not protected, without firstly seeking permission from the IT Department or the data protection lead within your setting or Head Office.

14.7 **Appropriate security measures** must always be taken. This includes making sure that the firewall on your device is enabled and using anti-virus software. Any software or operating system on your device must be kept up to date by promptly installing updates when they become available. You must make sure that you are using an operating system which is still supported (so you mustn't use an old version of Windows, such as Windows XP, for example).

14.8 **Default passwords**: If you use a personal device for work which came with a default password then this password must be changed immediately. See above for guidance on choosing a strong password.

14.9 **Sending or saving documents to your personal devices:** Documents containing Personal Data (including photographs and videos) must not be sent to or saved to personal devices, unless you have been given permission by the IT Department or the data protection lead within your setting or Head Office. 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 work 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.

14.10 **Friends and family:** You must not share work related Personal Data with your friends and family. For example, you must not share the login details with others and you must log out of your account once you have finished working. You must also make sure that your devices are not configured in a way that would allow someone else access to work related documents and information – if you are unsure about this then please speak to the IT Department or the data protection lead within your setting or Head Office. Disclosing work related Personal Data to your friends and family is a data breach, and if you do so knowingly or recklessly, it will also be a criminal offence. ILG is likely to consider breaches of confidentiality as a disciplinary matter.

14.11 **Social media:** You must never upload or publish work information using your personal social media account, even if your account is set to private. For example, you must not upload photographs of pupils under any circumstances.

14.12 **When you stop using your device for work:** If you stop using your device for work, for example if:

14.12.1 you decide that you do not wish to use your device for work; or

14.12.2 ILG withdraws permission for you to use your device; or

14.12.3 you are about to leave ILG

then, all work documents (including work emails), and any software applications provided by ILG for work purposes, must 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 ILG in relation to this process.

15 Breach of this policy

15.1 Any breach of this policy will be taken seriously, and may be treated as misconduct. This could result in disciplinary action including in serious cases, dismissal.

15.2 A member of staff who deliberately or recklessly obtains or discloses Personal Data held by ILG (or procures its disclosure to another person) without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal. In some cases, it can also be an offence to re-identify information which has been de-identified.

15.3 Further information on disciplinary procedures can be found in the ILG Employment Manual.

16 Version control

Date of adoption of this policy	February 2021
Date of last review of this policy	August 2024
Date for next review of this policy	August 2027
Policy owner	ILG Head Office