Data Protection Policy for Staff

Inspired Learning Group

February 2021

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). This policy has been drafted for all staff and therefore provides accessible and practical guidance. However, it does not cover the legislation in the level of detail which should be known to those at ILG who have a specific data protection compliance role. The policy directs staff to Head Office for additional guidance where this is required.

Contents

1 Introduction

1.1 This policy is about staff obligations under the data protection legislation. Data protection is about regulating the way that ILG uses and stores information about identifiable people (Personal Data). Data protection legislation also gives people various rights regarding their data - such as the right to access the Personal Data that ILG holds on them.

1.2 All ILG settings (including Head Office) collect, store and process Personal Data about staff, pupils, parents, suppliers and other third parties. It is recognised that the correct and lawful treatment of this data will maintain confidence in ILG and will ensure that ILG operates successfully.

1.3 All staff are obliged to comply with this policy when using Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.4 Head Office is responsible for helping staff to comply with ILG's data protection obligations. All queries concerning these matters should be raised with a member of the Data Protection Team.

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

3 What information falls within the scope of this policy

3.1 Data protection concerns information about individuals.

3.2 Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

3.3 Information as simple as someone's name and address is their Personal Data.

3.4 Examples of places where Personal Data might be found are:

3.4.1 on a computer database;

3.4.2 in a file, such as a pupil report;

3.4.3 a register or contract of employment;

3.4.4 pupils' exercise books, coursework and mark books;

3.4.5 health records; and

3.4.6 email correspondence.

3.5 Examples of documents where Personal Data might be found are:

3.5.1 a report about a child protection incident;

3.5.2 a record about disciplinary action taken against a member of staff;

3.5.3 photographs of pupils;

3.5.4 records of a job interview;

3.5.5 contact details and other personal data held about pupils, parents and staff and their families;

3.5.6 contact details of a member of the public who is enquiring about placing their child at a school or nursery;

3.5.7 financial records of a parent;

3.5.8 information on a pupil's performance; and

3.5.9 an opinion about a parent or colleague in an email.

3.6 These are just examples - there may be many other things that are used and created that would be considered Personal Data.

3.7 **Categories of Sensitive Personal Data:** The following categories are referred to as **Sensitive Personal Data** in this policy and in the Information Security Policy. Due to the nature of the Data, specific care must be taken in the following areas:

3.7.1 information concerning child protection or safeguarding matters;

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

3.7.3 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);

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

3.7.5 information about an individual's racial or ethnic origin;

3.7.6 religious beliefs or other beliefs of a similar nature;

3.7.7 physical or mental health or condition;

3.7.8 sex life or sexual orientation;

3.7.9 genetic information;

3.7.10 information relating to actual or alleged criminal activity; and

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

4 Staff obligations

4.1 **Our lawful bases for using your personal data are as follows:**

4.1.1 **Contract**: We need to use your information in order to comply with our contractual obligations and for you to perform your obligations as well. If we do not have a contract with you, for example if you are a volunteer, we will not rely on the contractual basis to use your information.

4.1.2 **Legitimate interests**: This means that ILG is using your personal data where this is necessary for ILG's legitimate interests or someone else's legitimate interests. Specifically,

ILG has a legitimate interest in educating and looking after its pupils, complying with its agreement with parents for their child to be at the School or Nursery, making sure that we are able to enforce our rights against you, for example, so that we take disciplinary action where appropriate, investigating if something has gone wrong and protecting ILG.

4.1.3 **Public task:** This allows ILG to use personal data where doing so is necessary in order to perform a task in the public interest. This basis applies when ILG is using personal data in order to educate and look after its pupils.

4.1.4 **Legal obligation**: As a School we have to comply with various laws and this entitles us to use your information where necessary. For example to fulfil our safeguarding duties towards pupils.

4.1.5 **Vital interests:** In limited circumstances we may use your information to protect your vital interests or the vital interests of someone else. For example, to prevent someone from being seriously harmed or killed.

4.2 **Personal Data must be processed fairly, lawfully and transparently**

4.2.1 What does this mean in practice?

(a) "Using" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

(b) People must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (the data protection regulator).

This information is provided in a document known as a privacy notice. Copies of ILG's privacy notices can be obtained from a member of the Head Office Data Protection Team. Staff should be aware of the contents of the privacy notice.

(c) If Personal Data is being used in a way which an individual might think is unfair, staff should speak to a member of the Head Office Data Protection Team.

(d) Personal Data must only be processed for the following purposes:

(i) ensuring that ILG provides a safe and secure environment;

(ii) providing pastoral care;

(iii) providing education and learning for pupils;

(iv) providing additional activities for pupils and parents (for example activity clubs);

(v) protecting and promoting ILG's interests and objectives (for example fundraising);

(vi) safeguarding and promoting the welfare of pupils; and

(vii) to fulfil ILG's contractual and other legal obligations.

(e) If specific consent of the individual is required to use their Personal Data, this must meet certain requirements. Staff must therefore speak to a member of the Head Office Data Protection Team if consent may be needed.

4.3 **Personal Data must only be processed for specified, explicit and legitimate purposes.**

4.3.1 What does this mean in practice?

(a) For example, if pupils are told that they will be photographed to enable staff to recognise them when writing references, these may not be used for another purpose (e.g. in ILG's prospectus). Staff should refer to ILG's Code of Conduct and the Guidance for Staff on the use of Photographs and Videos of Pupils by ILG for further information relating to the use of photographs and videos.

4.4 **Personal Data held must be adequate and relevant for the purpose**

4.4.1 What does this mean in practice?

(a) This means not making decisions based on incomplete data. For example, when writing reports, relevant information about the pupil should be used.

4.5 **Excessive or unnecessary Personal Data must not be held**

4.5.1 What does this mean in practice?

(a) Personal Data must not be processed in a way that is excessive or unnecessary. For example, information about a pupil's siblings may only be collected if that Personal Data has some relevance, such as a sibling fee discount being applicable.

4.6 **Personal Data held must be accurate**

4.6.1 What does this mean in practice?

(a) Personal Data must be complete and kept up to date. For example, if a parent advises that their contact details have changed, the management information system (MIS) must be updated.

4.7 **Personal Data must not be kept longer than necessary**

4.7.1 What does this this mean in practice?

(a) A policy is in place which outlines how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. Staff need to be aware of the contents of this policy, especially if this is part of their role. Particular care must be taken when deleting data.

(b) If guidance on retention periods and secure deletion is needed, staff should speak to a member of the Head Office Data Protection Team.

4.8 **Personal Data must be kept securely**

4.8.1 Staff must comply with the following policies and guidance relating to the handling of Personal Data:

(a) Information security policy;

(b) Guidance for Staff on the use of Photographs and Videos of Pupils by ILG;

(c) IT acceptable use policy for staff; and

(d) Information and records retention policy.

4.9 **Personal Data must not be transferred outside the EEA without adequate protection**

4.9.1 What does this mean in practice?

(a) If personal data needs to be transferred outside the EEA, staff should contact a member of the Head Office Data Protection Team. For example, if a school trip is being arranged to a country outside the EEA.

4.10 **Accountability**

4.10.1 ILG is responsible for and must be able to demonstrate compliance with the data protection principles. All staff are responsible for understanding their particular responsibilities under this policy to help ensure that accountability requirements are met.

4.11 **What personal data do we hold about you and how is this obtained?**

4.11.1 Information about you is gathered during the recruitment process for example: information about your education, qualifications and professional achievements, information provided on your application form and during interviews, information from your professional and social media profiles. Also when we receive your personal data (from you and third parties) in carrying out pre-employment checks, for example, when we receive references, confirmation of your fitness to work, your right to work in the UK and criminal records checks.

4.11.2 We will hold information about your performance. This includes information about skills, achievements, career progression, performance and disciplinary related matters.

4.11.3 We hold and use your financial information such as your bank details, your salary and pension details.

4.11.4 We will hold information about your We will hold information about your performance. This includes information about skills, achievements, career progression, performance and disciplinary related matters.

4.11.5 We will hold information about any physical or mental health condition you may have which is disclosed to ILG during the recruitment process or at any other stage of your involvement with ILG.

4.11.6 Your personal data will be created internally by ILG during the course of your employment or whilst you are volunteering with ILG. An email from the Head to a member of staff complimenting them on class management would be an example of this.

4.11.7 Your personal data may be acquired from outside of the ILG community such as from occupational health practitioners or from public authorities such as the Police or the Local Authority Designated Officer.

4.11.8 Your personal data will be held on ILG's Single Central Register and in staff files.

4.11.9 CCTV is used to make sure the School or Nursery site is safe. CCTV may be monitored by external contractors for security and welfare purposes. CCTV is not used in private areas such as changing rooms or toilets. See Appendix 1 for further details.

4.11.10 The use of door access systems may obtain data about staff attendance.

4.11.11 Vehicle tracking systems are used on company vehicles.

5 Sharing Personal Data outside ILG - dos and don'ts

5.1 Staff must be aware of the following dos and don'ts:

5.1.1 **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of ILG - if in doubt - always ask your Data Protection Co-ordinator.

5.1.2 **DO** encrypt emails which contain Critical School Personal Data described in paragraph 3.7 above. For example, encryption must be used when sending details of a safeguarding incident to social services.

5.1.3 **DO** make sure that permission is sought from your Data Protection Co-ordinator or member of the Head Office Data Protection Team to share Personal Data on the ILG or setting website.

5.1.4 **DO** share Personal Data in accordance with ILG's Safeguarding policy and procedures. If there are any questions or concerns relating to safeguarding, contact your Designated Safeguarding Lead.

5.1.5 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. Advice must be sought from your Data Protection Co-ordinator or member of the Head Office Data Protection Team where there is suspicion as to why the information is being requested or if there is uncertainty regarding the identity of the requester (e.g. if a request has come from a parent but using a different email address).

5.1.6 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. **DO NOT** reply to email, text, or pop-up messages that ask for personal or financial information, or click on any links in an email from an unrecognised person. All concerns about phishing must be reported to a member of the Head Office Data Protection Team immediately.

5.1.7 **DO NOT** disclose Personal Data to the Police without permission from a member of the Head Office Data Protection Team (unless it is an emergency).

5.1.8 **DO NOT** disclose Personal Data to contractors without permission from a member of the Head Office Data Protection Team. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil recruitment event.

6 Accessing or sharing Personal Data within ILG

6.1 This section applies when Personal Data is accessed or shared within ILG.

6.2 Personal Data must only be accessed or shared within ILG on a "need to know" basis.

6.3 Examples which are **likely** to comply with data protection legislation:

6.3.1 a teacher discussing a pupil's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil);

6.3.2 sharing Personal Data in accordance with ILG's Safeguarding policy;

6.3.3 informing an exam invigilator that a particular pupil suffers from panic attacks; and

6.3.4 disclosing details of a teaching assistant's allergy to bee stings to colleagues so that staff will know how to respond (but more private health matters must be kept confidential).

6.4 Examples which are **unlikely** to comply with data protection legislation:

6.4.1 the Head or Nursery Manager being given access to all records kept by nurses working within the setting (seniority does not necessarily mean a right of access);

6.4.2 a member of staff looking at a colleague's HR records without good reason. For example, if they are being nosey or suspect their colleague earns more than they do. In fact accessing records without good reason can be a criminal offence (see paragraph 10.2 below).

6.4.3 informing all staff that a pupil has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil); and

6.4.4 disclosing personal contact details for a member of staff (e.g. their home address and telephone number) to other members of staff - unless the member of staff has given permission or it is an emergency.

6.5 Personal Data may be shared to avoid harm, for example in child protection and safeguarding matters. Staff would have received training on when to share information regarding welfare and safeguarding issues. If this training has not been provided, contact your Designated Safeguarding Lead as a matter of urgency.

6.6 Where you are employed by us in order to fulfil our obligations to you as an employer we will need to share your information with medical professionals, such as occupational health services, where we are making a referral.

6.7 If ILG is dealing with a complaint or grievance (e.g. from a colleague or a parent), we will need to share your information with other parties if it is relevant, for example, the appropriate staff at ILG, the colleague or parents making the complaint.

6.8 We may need to share your information if there is an emergency, for example, if you are hurt in an accident.

7 Individuals' rights in their Personal Data

7.1 People have various rights in their information.

7.2 Staff must be able to recognise when someone is exercising their rights, so that the matter can be referred. These rights can be exercised either in writing (e.g. in an email) or orally.

(a) Your Data Protection Co-ordinator must be informed if anyone (either for themselves or on behalf of another person, such as their child):

(i) wants to know what information ILG holds about them or their child;

(ii) asks to withdraw any consent that they have given to use their information or information about their child;

(iii) wants ILG to delete any information;

(iv) asks ILG to correct or change information (unless this is a routine updating of information such as contact details);

(v) asks for personal data to be transferred to them or to another organisation;

(vi) wants ILG to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the ILG newsletter or alumni events information; or

(vii) objects to how ILG is using their information or wants ILG to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party.

(b) Please note, a person may be committing a criminal offence if they alter, block, erase, destroy or conceal information to prevent it from being disclosed (for example, to prevent its disclosure if a subject access request for that information has been received). Therefore if information or documents are requested by a colleague at ILG who is preparing a response to a request for information, everything must be provided.

8 Requests for Personal Data (Subject Access Requests)

8.1 One of the most commonly exercised rights mentioned in section 7 above is the right to make a subject access request. Under this right people are entitled to request a copy of the Personal Data which ILG holds about them (or in some cases their child) and to certain supplemental information.

8.2 Subject access requests do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. Always immediately let a member of the Head Office Data Protection Team know if those requests are received.

8.3 Receiving a subject access request is a serious matter for ILG and involves complex legal rights. Staff must never respond to a subject access request themselves unless authorised to do so.

8.4 When a subject access request is made, ILG must disclose all of that person's Personal Data to them which falls within the scope of their request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request. However, this must not deter staff from recording and passing on information where this is appropriate to fulfil any professional duties, particularly in relation to safeguarding matters.

9 For how long does ILG keep staff personal data?

9.1 We keep your information for as long as we need to in relation to your employment. We will keep some information after you have left ILG in case this is needed, for example, in relation to our legal obligations.

9.2 In some cases we may keep your information for a longer time than usual but we would only do so if we had a good reason and only if we are allowed to do so under Data Protection Law.

10 Breach of this policy

10.1 A breach of this policy may be treated as misconduct and could result in disciplinary action including in serious cases, dismissal.

10.2 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. In some cases, it can also be an offence to re-identify information which has been de-identified. Staff should speak to a member of the Head Office Data Protection Team before doing this.

11 Version control

Date of adoption of this policy	22 February 2021
Date of last review of this policy	22 February 2021
Date for next review of this policy	February 2024
Policy owner	Head Office

Appendix 1 - CCTV

1 The use of CCTV

1.1 CCTV systems are used on all ILG premises. These consist of a number of cameras on each site.

1.2 CCTV is used to safeguard the welfare of pupils, staff and visitor; to protect ILG, pupils, parents, staff and visitors from criminal activity such as theft and vandalism; to increase personal safety; to support the protection of property; to aid in the investigation of accidents and incidents and the monitoring of health and safety; and to support law enforcement agencies in the reduction, prevention and detection of crime and to assist in the identification, apprehension and potentially prosecution of offenders.

1.3 CCTV footage may contain the personal information of those individuals captured by the recording.

2 Minimising privacy risks

2.1 The use of CCTV is deemed a necessary and proportionate measure to achieve the purposes listed above.

2.2 ILG will review its use of CCTV should a concern be raised about its practices.

3 The operation of CCTV

3.1 ILG has sited the cameras to view only areas which need to be monitored, for example, they do not monitor neighbouring private residences.

3.2 Where CCTV cameras are placed on ILG premises, signs are displayed to alert individuals that their image may be recorded. These will identify ILG as the organisation operating the system, identify the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

3.3 CCTV is not used in areas where individuals will have a heightened expectation of privacy, for example, there are no cameras in toilets or changing rooms.

3.4 The cameras have been positioned in a way to ensure their security and to protect them from vandalism. They are designed to produce images of the necessary clarity and quality to meet ILG's purposes.

3.5 Images can be extracted from the system if required, for example, under a disclosure to law enforcement agencies and or under a subject access request (please see section 9 for more information on subject access requests). ILG is able to obscure parts of the images where required to protect the identity of individuals.

3.6 The CCTV does not capture sound recordings.

3.7 The CCTV cameras which record the perimeter of the School sites are usually in operation 24 hours a day every day of the year, because this is necessary to meet the purposes for which they were installed (for example, to detect intruders).

3.8 ILG is responsible for the operation of all CCTV in accordance with this policy for the purposes identified above.

3.9 ILG will not engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or equivalent serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

3.10 In the unlikely event that covert monitoring is considered to be justified, ILG will carry out a Data Protection Impact Assessment. The rights of individuals whose images may be captured will always be taken into account in reaching any such decision.

4 Management and maintenance of CCTV equipment

4.1 CCTV equipment is managed and maintained by an appointed contractor, including any software updates that may be required. Any concerns or defects should be reported directly to them.

5 Storage and security

5.1 CCTV footage will be stored securely, and will only be accessed by designated ILG staff and appointed contractor.

5.2 CCTV recordings, including any copies made, are encrypted. ILG will also encrypt any copy before it is shared with a third party (such as a law enforcement agency) unless there is a good reason for not doing so.

5.3 Any information security breach (for example, any unauthorised access to CCTV footage) must be reported immediately to the Data Protection Co-ordinator.

5.4 Where footage is saved following an incident this will be done securely.

6 Internal use of the CCTV

6.1 If a member of staff considers that CCTV footage might be needed for an internal matter (e.g. a disciplinary issue) they should speak to the Data Protection Co-ordinator in the first instance.

7 Retention

7.1 Compliance with data protection law means that ILG does not retain personal data for longer than is required for the purposes for which it was obtained. Recorded images will normally be retained for 90 days from the date of recording, in accordance with the Information and Records Retention Policy.

8 Informing individuals about the use of CCTV

8.1 ILG appreciates the importance of being open and transparent about the use of CCTV. This policy is published on ILG's website and is available on request from Head Office.

8.2 ILG's privacy notices for parents and pupils includes information about the use of CCTV by ILG. These are available on the individual school or nursery website.

9 Subject access requests

9.1 Under data protection legislation individuals have the right to access information about themselves which may include images of them in CCTV footage.

9.2 Any subject access requests must be made to the Data Protection Co-ordinator.

10 Disclosure to law enforcement agencies

10.1 Images from the CCTV system may be disclosed to law enforcement agencies (e.g. the Police) where ILG considers such disclosure necessary (for example, for the prevention and detection of crime). However, any such disclosure will only be in accordance with data protection law.

10.2 Any requests from law enforcement agencies should be referred to the Data Protection Co-ordinator.

11 Other requests for information

11.1 CCTV footage may be disclosed in other circumstances if this is in accordance with data protection legislation. For example, if required by a court order or if in connection with legal proceedings.

11.2 Applications received from outside bodies (e.g. solicitors) to view footage must be referred by staff to the Data Protection Co-ordinator.

11.3 CCTV footage will not be made available to the media for commercial or entertainment purposes.

11.4 Records will be maintained of all disclosures of CCTV footage.

12 Contractors (also known as Processors)

12.1 ILG is required to have a written agreement in place with any organisation which handles the CCTV footage on its behalf (known as processors).

13 Breaches of this policy

13.1 If staff consider that this policy is not being followed in any respect, they must inform the Data Protection Co-ordinator.

13.2 Any breach of this policy by a member of staff will be taken seriously and may result in disciplinary action.

14 Legal basis for processing

14.1 ILG considers that there is a legitimate interest in using CCTV for the purposes described above. In addition, anyone attending their premises also has a legitimate interest (ie. so that they are confident that the sites are safe). ILG considers that CCTV is necessary, and that they are being used fairly. The use of CCTV is also in the public interest.

Appendix 2 – Website privacy

1 Introduction

1.1 Website privacy applies to users of all ILG websites (including the individual schools & nurseries), as well as any person who provides services to us – either as an individual, employee or representative of a corporate service provider.

2 Information that is collected and processed

2.1 ILG collects personal data directly from you when you enquire about our products and services, or where ILG enters into a contract to receive services from you or when you use our sites. Information may also be gained from your employer or colleagues. Information may be collected during the period of our relationship.

2.2 Personal data may be used to carry out obligations arising from any contracts between us and you, with our customers, with suppliers, or with third parties; to communicate with you, including to provide you with information, products or services; and where it is necessary for our business or our customers' business.

3 Legal basis for processing

3.1 ILG considers that there is a legitimate interest for collecting personal data. These may include your name, job title, email address, telephone number and address (including bank details if applicable). This is necessary for performance of the contract between us, to manage our relationship with you, to fulfil our obligations, to provide you with purchases, to capture your preferences, to collect technical information, to perform due diligence and to enforce our legal rights.

3.2 Feedback may be provided to you on our products and services, which is necessary to improve them.

3.3 ILG may contact you about our products and services by email, telephone, post or by text message, but only where we are allowed to under data protection law. If you tell us that you do not want to be contacted for any of these purposes then of course that will be respected. Sometimes we will need your consent before contacting you for these reasons. If you give us your consent then you have a right to withdraw that consent at any time. Any use of your personal data before you withdraw consent remains valid.

4 Sharing information

4.1 Your information may be shared with third parties where required by law, where it is necessary to administer the working relationship with you or where there is another legitimate interest or legal obligation in doing so. This includes third party service providers who act on our behalf.

4.2 If ever in the future, ILG is considering restructuring or selling our business, your information may be shared with the other parties involved and with the relevant professional advisors. This is for our legitimate interest in making sure that potential buyers and partners have the information they need about ILG.

5 Retention

5.1 Personal data is usually only retained for as long as necessary to fulfil the purposes it was collected for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

5.2 To determine the appropriate retention period for personal data, ILG considers the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which your personal data is being processed, and whether this can be achieved through other means, and the applicable legal requirements.

5.3 For anyone who has a contract with ILG, information is typically kept for six or twelve years after the contract is finished. This does not apply to any parental contracts for the education of their children.

6 Website cookies

6.1 Cookies are used in order to improve your experience of our websites, and for their improvement. When accessing our websites, a message will appear at the bottom of the home page stating that the site uses cookies. For further details, select ‘Find out more’.

Appendix 3 – Data breaches

1 Introduction

1.1 ILG understands the importance of keeping personal data secure and of effectively dealing with data breaches. This is essential for maintaining the trust of staff, pupils and parents when ILG uses their information.

1.2 In the event of a data breach, the policy on Information Security will be applied. This document outlines brief procedures for staff on how to recognise and deal with a data breach.

1.3 ILG is required to report certain breaches to the Information Commissioner's Office (ICO) and to data subjects under the General Data Protection Regulation (GDPR). There are strict timescales for reporting breaches, which are outlined in the Information Security policy.

2 Immediate action following a data breach

- Inform the Chief Privacy Officer.
- The Data Protection Co-ordinator and Chief Privacy Officer will work together to Identify what personal data is at risk, and what measures can be taken to prevent the breach from worsening, eg. changing passwords / access codes, segregating the information held on ILG's systems.
- They will arrange for any compromised data to be recovered, with the assistance of ILG's IT consultants, for example use backups to restore data.
- The Chief Privacy Officer will consider whether outside agencies need to be informed as a matter of urgency e.g. the police in the event of a burglary or Children's Services where the breach may lead to serious harm being caused to a pupil.
- The Chief Privacy Officer will consider whether any affected individuals should be told about the breach straight away. For example, so that they may take action to protect themselves or because they would find out about the breach from another source. This is different to the mandatory notification to individuals, which does not need to be an immediate notification.

3 What is a data breach?

3.1 A data breach is a breach of security which leads to the loss of personal data; the accidental or unlawful destruction of personal data; the disclosure of personal data to an unauthorised third party; the unlawful or accidental alteration of personal data; or unauthorised access to personal data.

3.2 Personal data is information:

3.2.1 from which a living person can be identified (either from the information itself or when combined with other information likely to be used to identify the person); and

3.2.2 which relates that person.

3.3 The following are examples of personal data held by ILG:

3.3.1 names and contact details of pupils, parents and staff;

3.3.2 financial information about parents and staff;

3.3.3 pupil exam results;

3.3.4 safeguarding information about a particular family;

3.3.5 information about pupil behaviour and attainment; and

3.3.6 a pupil or staff member's medical information.

3.4 If staff are in any doubt as to whether an incident constitutes a data breach, they must speak to their Data Protection Co-ordinator immediately, who will inform the Chief Privacy Officer.

Appendix 4 - Data Protection Team

Data Protection Team