Lapwing

General Data Protection Regulation (GDPR) Policy

Lapwing's commitment
Lapwing is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the General Data Protection Regulation (GDPR) which came into force on 25th May 2018. https://ico.org.uk/for-organisations/

Changes to data protection legislation shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows:
(a) Consent: the member of staff/student/parent/carer has given clear consent for Lapwing to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.
(c) Legal obligation: the processing is necessary for Lapwing to comply with the law (not including contractual obligations).

The member of staff responsible for data protection is:
Will Fletcher, Data Protection Officer (DPO)
wfletcher@lapwingeducation.com
07501 969099 / 01473 621762

However, all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

Lapwing is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through on-going training in this area and as part of the induction process. This is recorded in the staff training record log.

The requirements of this policy are mandatory for all staff (including employees and volunteers) employed by Lapwing and any third party contracted to provide services to Lapwing.

Personal and sensitive data
All data within Lapwing's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The principles of the General Data Protection Regulation shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure

- ensure that data is not transferred to other countries without adequate protection.

Fair processing / privacy notice
We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and students prior to the processing of an individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'children' under the legislation.

There may be circumstances where Lapwing is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, social care, or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of Lapwing shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of an individual's data shall first be notified to them or their parent/carer. Under no circumstances will Lapwing disclose information or data:

- that would cause serious harm to the student or anyone else's physical or mental health or condition
- indicating that the student is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the Lapwing or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent.

Data security
In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Data Protection Impact Assessments shall be conducted in accordance with guidance given by the ICO: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. The DPO will be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Thrive online is a third-party organisation who process our students' data for the purpose of delivering the intervention and monitoring impact. This is via a secure cloud-based platform and we have a 'multi-user subscription services agreement' with them that details GDPR compliancy.

The Minding the Gap project funded by the Big Lottery and European Social Fund has a separate Privacy Notice (see Appendix 8), which all MTG staff have signed. All key workers will carry a copy of this to make new participants aware of the notice.

Personal data about students will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

- Other educational or care settings. If a student transfers from Lapwing to another setting, their academic records and other data that relates to their health and welfare will be forwarded onto the new school/setting. This will support a smooth transition from one setting to the next and ensure that the student is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the student's academic and emotional progress as a result of the move.
- Examination authorities, this may be for registration purposes, to allow the students at Lapwing to sit examinations set by external exam bodies.
- Health authorities, as obliged under health legislation, Lapwing may pass on information regarding the health of students to monitor and avoid the spread of contagious diseases in the interest of public health.
- Police and courts, if a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- Social workers and support agencies, in order to protect or maintain the welfare of our students, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Right to be forgotten: Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by Lapwing including any data held by contracted processors.

Photographs and video

Images of staff and students may be captured at appropriate times and as part of educational activities for use internally by Lapwing only.

Unless prior consent from parents/carers/students/staff has been given, Lapwing shall not utilise such images for publication or communication to external sources.

It is Lapwing's policy that external parties may not capture images of staff or students without prior consent.

Location of information and data

Any existing hard copy data will be scanned onto the secure cloud and hard copies shredded. The exception to this is safeguarding information on students, hard copies are kept in a locked drawer. Sensitive or personal information and data should not be removed from the Lapwing office, however Lapwing acknowledges that some staff may need to transport data between sessions and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings or are on visits or sessions with students. Such data will be kept with the member of staff or left in a secure place which cannot be accessed by others.

The majority of data is stored on our secure cloud which can be accessed by staff at home. The cloud has restricted access for different members of staff. This is managed by Lucid Systems. Staff will have work laptops encrypted and any staff using their own laptops for work will need to provide evidence of encryption on the laptop.

We have no archived paperwork, as this was securely shredded by an external company in September 2018. All archived documents are stored within the cloud.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should be kept with staff. The information should not be on view in public places or left unattended under any circumstances.

- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or student by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.
- Any documentation created relating to a student should be accessed and stored only on the secure cloud. All Lapwing laptops are encrypted. Staff without a Lapwing laptop access the cloud through an encrypted USB, which ensures no data is stored on their own laptop. Lucid Systems manage the storage and security of the cloud. They are available during office hours to support staff with any issues around access.
- External emails that contain sensitive data or files on a student or member of staff must be sent with password protection, unless sending to a secure and known email address. The password must be supplied to the recipient of the email by other means eg. A text or phone call and must not be sent via the same email address.
- Mobile phones used for any Lapwing work will have a 6 digit passcode applied (not a date of birth!) Both android and IOS phones have a function where if an incorrect passcode is entered so many times it will shut down or reset the phone. Staff will ensure that this is set. An auto-lock will be applied when the screen automatically switches off. 'Find my device' setting is to be switched on to locate the phone if lost. Staff will ensure their mobile cannot be accessed by students or by family members.

These guidelines are clearly communicated to all Lapwing staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

When staff leave Lapwing their email and cloud access will be shut down promptly by Lucid.

Data retention and disposal
Lapwing will hold staff data for six years after their termination of employment in line with guidance from the IRMS toolkit: http://irms.org.uk/page/SchoolsToolkit. Using the same guidance we will be passing on student data held to their next education provider and Lucid IT will then securely delete the file we hold. If we are the last education provider then we will keep personal data until their DOB +25 years.

All paper archives were securely shredded by an external company in September 2018. Staff will shred any paper documentation after uploading to the cloud.

Disposal of IT assets holding data shall be in compliance with ICO guidance: https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The Data Protection Officer has responsibility for the GDPR compliancy plan. If you wish to view this please contact the DPO.

Appendices
Appendix 1. Data Breach Procedure
Appendix 2. Privacy Statement (Student)
Appendix 3. Privacy Statement (Staff)
Appendix 4. Schools Choice Incident Grading Document
Appendix 5. Schools Choice Data Classification Document
Appendix 6. Data Protection Officer Job description
Appendix 7. Lapwing Data Consent Form
Appendix 8. Minding The Gap Privacy Statement

Author:	**Will Fletcher**
Issued:	**1 September 2022**
Approved:	**30 August 2022**
Next review:	**August 2024**

Lapwing

Appendix 1

Data Breach Procedure

Important note: This procedure has been produced based on current General Data Protection Regulations (GDPR) information. As further updates are released this procedure may be updated to reflect the changes. The GDPR has applied in the UK from 25 May 2018.

Policy statement
Lapwing holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Lapwing and all staff, trustees, volunteers and contractors, referred to herein after as 'staff'.

Purpose
This breach procedure sets out the course of action to be followed by all staff at Lapwing if a data protection breach takes place.

Legal context
Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of breach
Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of student, staff or trustee data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a data breach
In the event that Lapwing identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Lapwing's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant parties such as Lucid Systems.

3. The DPO (or nominated representative) must inform the CEO as soon as possible. As a registered Data Controller, it is Lapwing's responsibility to take the appropriate action and conduct any investigation.

4. The DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from legal support should be obtained.

5. The DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

    a. Attempting to recover lost equipment.

    b. Consideration should be given to a global email to all Lapwing staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the DPO (or nominated representative).

    c. The use of back-ups to restore lost/damaged/stolen data.

    d. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

    e. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation
In most cases, the next stage would be for the DPO (or nominated representative) to fully investigate the breach. The DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:
- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;

- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (students, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification
Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what Lapwing is able to do to help them. Lapwing will also give them the opportunity to make a formal complaint if they wish (see Lapwing's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation
Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. Disciplinary action may be taken against staff members involved. An update should be reported to the next available Senior Management Team and Trustees meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation
The DPO should ensure that staff are aware of Lapwing's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the Lapwing's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or CEO/Head of Education.

See documents 'Schools Choice Template Incident Grading Document' and 'School Choice Data Classification Document' to support our Data Breach Procedure.

Lapwing

Appendix 2

Privacy Notice (How we use student information)

The categories of student information that we collect, hold and share include:

- Personal information (such as name, address)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Correspondence with other agencies and settings involved in the education, health or social care of that student
- Records from previous or other current provisions (such as SEND records, risk assessments, referral information, qualifications)
- Information gathered by staff (such as assessment information, session plans and evaluations, risk assessments, programme plans, exam papers)

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to share information with other agencies working with the student (such as the Local Authority, social care, health services, schools and colleges)
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We collect and use pupil information under Article 6(1) from the GDPR – 'consent' and from Article 9(2) 'explicit consent' to process special category (sensitive) personal data.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

Any student moving on to another educational provision will have all their data forwarded securely on to that setting and this will be documented. For students who do not continue onto another provision or setting we will keep documentation in line with the Information and Record Management Society (IRMS) and Limitation Act 1980 up to the Date of Birth of the pupil +25 years, before deleting from our secure data drive. Previous students will have their archived electronic files dated when they will be deleted according to their date of birth +25 years. All hard copies will be securely disposed of as information is held electronically on the secure data drive.

Who we share student information with

We routinely share student information with:

- parents/carers
- settings that our students are on roll with
- settings that the students attend after leaving us
- the local authority, social care, health
- Thrive online (students accessing this intervention)

For any other parties we will communicate this to the student/parent/carer.

Why we share student information
We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.
We share students' data with agencies and settings involved with the student to ensure effective multi-agency working to benefit the students.

Students aged 13+
Once students reach the age of 13, they should have had pupil information passed to their local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. If they haven't this is something we can do.
This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age of 16.

Pupils aged 16+
Certain information about pupils aged 16+ is shared with their local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. Lapwing can do this if it has not previously been done.
This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit the appropriate local authority website.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

The Minding the Gap project funded by the Big Lottery and European Social Fund has a separate Privacy Notice. All key workers will carry a copy of this to make new participants aware of the notice.

Contact
If you would like to discuss anything in this privacy notice, please contact:
Will Fletcher (Data Protection Officer)
wfletcher@lapwingeducation.com or 01473 621762 / 07501 969099

Lapwing

Appendix 3

Privacy Notice (How we use staff information)

The categories of Lapwing workforce information that we collect, process, hold and share include:

- personal information (such as name, address, phone numbers, national insurance number)
- special categories of data including characteristics information such as gender and age
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications
- car insurance documents
- bank account details
- Performance information

Why we collect and use this information

We use workforce data to:

- perform safer recruitment due diligence
- enable the development of a comprehensive picture of the workforce and how it is deployed
- enable individuals to be paid
- staff development and monitoring

The lawful basis on which we process this information

We process this information under article 6(1) from the GDPR a) 'consent' and f) 'legitimate interests' from Article 9(2) a) 'explicit consent' and b) 'necessary for carrying out obligations'**.**

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain staff workforce information to us or if you have a choice in this.

Storing this information

We hold your data under the Limitation Act 1980 for 6 years after the date your employment with us is terminated.

Who we share this information with

We only share information outside of Lapwing with the Third Parties: Lovewell Blake for payroll and FSB for pension contributions and any other organisation for the performance of the role or with consent to provide a reference.

Why we share workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact the DPO.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact:
Will Fletcher (Data Protection Officer)
wfletcher@lapwingeducation.com or 01473 621762 / 07501 969099

Lapwing

Appendix 4

Data classification

Classification	Description of Information Types
Green	No Impact - information formally made public by school or information which would have no impact on privacy or school reputation if it was to be put into the public domain by any other means.
Amber	Strictly internal or agreed partners - school information which is intended strictly for internal use by staff and agreed partners.
	Information posing little/no risk to privacy - this could also include names, addresses and pupil numbers that pose little or no risk to privacy.
Red / Offical – Sensitive	Health & care personal data - personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity, gender or sexuality.
	Financial personal data - personal data which reveals anything about the financial circumstances of any individuals or families.
	Employee & partner personal data - personal data on employees of the school and its partners. This includes details about ethnicity, gender or sexuality.
	Safeguarding information
	Impact on health, safety & wellbeing - anything which, if disclosed, would impact on the health, safety and wellbeing of people. This includes details about ethnicity, gender or sexuality.
	School information which would have a significant impact on the reputation or business of the school if it was seen by non-intended recipient because of commercial, legal, fraud, investigatory or other areas where confidentiality is necessary.

Lapwing

Appendix 5

Incident Grading For Data Breach

Incident grading 1 = Negligible
Any type of incident formally recorded, or something worthy of investigation but turns out to be a “false positive”, “near miss” or loss of equipment where there is a remote chance of the data being readable, which has negligible impact on privacy or school. **Reporting of such incidents is still valuable and should be used as part of ongoing information security risk assessment.*

Incident grading 2 = Minor	
Confidentiality	Confirmed or likely loss of personal data or other privacy breach relating to up to 10 individuals that poses low risk to privacy and no health or safety impacts (e.g. just name, address, pupil number at amber level)
Integrity	Confirmed or likely issues relating to integrity of information on <10 staff or pupils such as confused identities, out of date information or records misplaced which causes localised inconvenience or delays.
Availability	Some localised and short-lived loss of availability, such as through a temporary systems failure, which leads to the disruption of non-critical teams/areas.

Incident grading 3 = Moderate	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 10 individuals OR any breach of “OFFICIAL- SENSITIVE” information at red level. Likely local media interest and adverse publicity.
Integrity	Issues relating to integrity of information to the extent that the data can no longer be understood or is out of date and could have health, social care and safety or other implications.
Availability	Some disruption to critical services that means information is unavailable causing unacceptable impact and invocation of local team business continuity plans. This may be either a short disruption to a very critical team/area or a longer disruption to a group of less critical teams/areas.

Incident grading 4 = Major	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 100 individuals OR loss of any sensitive personal data at red level which is highly likely to affect the health or safety of one or more

Incident grading 5 = Extreme	
Confidentiality	Loss of data or privacy breach relating at large scale (i.e. 100,000+ persons or complete datasets); likely national/international media adverse publicity, prolonged damage (for example parent trust) and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc.
Integrity	Integrity problem which leads to significant amounts of data on 100,000+ persons being unreadable or unusable and does directly lead to health and safety issues or significant services issues (e.g. entire data set for pupil group corrupted beyond use that must be re-created).
Availability	Outage or other issue which leads to general failure of IT so that teams/areas which are critical to the school are not running for a prolonged period. Business Continuity Plans across school/trust are invoked.

Lapwing

Appendix 6

Data Protection Officer (DPO)

Job description

- Train the staff in data processing.
- Develop and execute relevant compliance projects.
- Conduct regular security audits to ensure compliance and address potential problems.
- Act as the point of contact between the company and any Supervisory Authorities (SAs).
- Give advice on the impact of data protection efforts.
- Monitor and maintain records of all data processing activities conducted by the company.
- Review the company's agreements and contracts with data processors.
- Communicate with data subjects to inform them about how their data is being processed and the rights they have to their data.
- Coordinate data breach response and notification procedures.

Job requirements

- Knowledge of data protection law and practices
- Knowledge of the company's IT infrastructure and organisational structure
- Align with the company's data processing operations and the level of data protection required for the company
- Write all policy documentation required and update as necessary
- Excellent management skills
- Excellent verbal and written communication

Lapwing

Appendix 6

Consent form for students and parents / carers.

Student name: _____

MEDIA CONSENT

All education delivery staff carry mobile phones with photo and video capabilities. This helps us to record students' achievements to help measure and evidence their progress.

To be completed by parent / carer OR by student if over 13 years old	Yes	No
I consent to photos of me / my child being taken during sessions to record progress		
I consent to video footage of me / my child being taken during sessions to record progress		
I consent to photos of me / my child being used in Lapwing publications and shared on the Lapwing website and social media		
I consent to video footage of me / my child's being used in Lapwing publications and shared on the Lapwing website and social media		
I consent to audio recordings of me / my child being used in Lapwing publications and shared on the Lapwing website and social media		
I consent to success stories written about me / my child being used in Lapwing publications and shared on the website and social media		

RELATIONSHIPS, SEX & HEALTH EDUCATION

Lapwing deliver a RSHE curriculum that is appropriate for the age and profile/needs of each student. Most, but not all, elements of this curriculum are compulsory. If you need more information, please see the information on our website in our Student Support Policy or contact us directly.

From the age of 16 years old students themselves can opt out of sex education. From three terms before their 16th birthday students can opt in even if their parent / carer wishes to withdraw them.

To be completed by parent / carer if student is under 16 years old	Yes	No
I consent to Lapwing teaching my child about intimate relationships, including sex education (appropriate to their age, needs and understanding)		

THRIVE APPROACH

At Lapwing we often use the Thrive Approach with our students. This helps young people with their emotional development. More information is available on our website.

To be completed by parent / carer OR by student if over 13 years old	Yes	No
I consent to Lapwing using the Thrive approach with me / my child		

AGREEMENT TO SHARE YOUR INFORMATION
We may need to share some of your personal information with other organisations so that they can help us to deliver the most appropriate and effective provision that you or your child need(s).

Declaration – to be completed by parent / carer OR student if over 13 years old:

☐ I understand that information is securely stored about me/my child. I have had the opportunity to discuss what this means and consider the content of Lapwing's Data Protection Policy.

☐ I agree that personal information about me/my child may be shared with other agencies and professionals.
Please indicate any exceptions
(If there are no exceptions, state NONE)

☐ I agree that you can contact other agencies and professionals who are or have been involved with me/my child and seek relevant information from them to decide what additional provision or support may be needed.
Please indicate any exceptions
(If there are no exceptions, state NONE)

Parent / carer(s) signature(s)

Signed…….…….. Name ……..……..……

Date…….…….....

Signed…….…….. Name ……..……..……

Date…….…….....

Signature of any other person with parental responsibility (PR)

Signed…….…….. Name ……..……..……

Role…….Date…….……..…....

Signature of young person if over 13 years of age and able to give consent.
I agree with all of the above consent.

Signed…….…….. Name ……..……..……

Date…….…….....

Should you wish to withdraw any of the above consent then you can do so at any time by emailing or writing to Kendra Collier, Norfolk (kcollier@lapwingeducation.com) or Lisa Squirrell, Suffolk & Essex (lsquirrell@lapwingeducation.com).

Address: Lapwing Education, 8a The Square, Martlesham Heath, Suffolk, IP5 3SL
Tel: 01473 621762

Appendix 8

Lapwing

Minding the Gap – Privacy Information Notice for Partners & Participants

What is the purpose of this document?

Minding the Gap is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship/project involvement with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all partners, their employees whose data we will hold, and participants of Minding the Gap.

As part of the national Building Better Opportunities programme and therefore led by the Managing Authority – Department for Work and Pensions, Participant personal data collected for ESF and BBO programmes is covered within the DWP Privacy notice. This can be found at www.gov.uk/dwp/personal-information-charter

Community Action Suffolk (Lead partner), Realise Futures, Lapwing Suffolk, and Access Community Trust (Area Coordination Partners) are "data controllers". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees of partner organisations and project participants. This notice does not form part of any contract of employment or other contract to provide services. Community Action Suffolk may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Delivery partners of the Minding the Gap project are “Data Processors” on our behalf and will comply with this notice in their processing of employee and participant data.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.

2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.

4. Accurate and kept up to date.

5. Kept only as long as necessary for the purposes we have told you about.

6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection.

We may collect, store, and use the following categories of personal information about you:

•Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses

•Date of birth

•Gender

•Marital status and dependants

•Next of kin and emergency contact information

•National Insurance number

•Bank account details, payroll records and tax status information

•Salary, annual leave, pension and benefits information

•Start date

•Location of employment or workplace

•Copy of identity documents – birth certificate, passport or driving licence

•Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process)

•Employment records (including job titles, work history, working hours, training records and professional memberships)

•Performance information

•Disciplinary and grievance information

•Information about your use of our information and communications systems

•Photographs

We may also collect, store and use the following "special categories" of more sensitive personal information:

•Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions

•Information about your health, including any medical condition, health and sickness records

•Information about criminal convictions and offences

How is your personal information collected?

We typically collect personal information about employees, and participants through the application and recruitment process, either directly from participants, or from MTG partner organisations during the claim process. We may sometimes collect additional information from third parties including referral agencies.

We will collect additional personal information in the course of job-related or project activities throughout the period of you working with us.

How we will use information about you

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal obligation.

3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).

2. Where it is needed in the public interest [or for official purposes].

Situations in which we will use your personal information

We need all the categories of information in the list above (see The kind of information we hold about you) primarily to allow us to perform our contract with you[*] and to enable us to comply with legal obligations[**]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties[***], provided your interests and

fundamental rights do not override those interests. The situations in which we will process your personal information are listed below. [We have indicated by [asterisks] the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of data are involved.]

- Making a decision about your recruitment and appointment. *
- Making a decision about your eligibility for the project in accordance with the EU eligibility regulations. *,**
- Determining the terms on which you work for and with us. *,**
- Checking you are legally entitled to work in the UK. **
- Paying you salary and/or expenses and, if you are an employee, deducting tax and National Insurance contributions. *,**
- Administering the contract we have entered into with you. *,**
- Project management and planning, including accounting and auditing. **,***
- Conducting performance reviews, managing performance and determining performance requirements.*,**
- Gathering evidence for possible grievance or disciplinary hearings.*,**
- Making decisions about your continued engagement with the project.*,**
- Making arrangements for the termination of our working relationship.*,**,***
- Education, training and development requirements.*,**
- Dealing with legal disputes involving you, or other employees, workers and contractors, including incidents/accidents in project time.*,**,***
- Ascertaining your fitness to work/take part in activities.*,**
- Complying with health and safety obligations.*,**,***
- To prevent fraud.*,**,***
- To monitor your use of our information and communication systems to ensure compliance with our project policies.*,**
- To ensure network and information security, including preventing unauthorised access to our networks and electronic communications systems and preventing malicious software distribution.*,**,***
- To conduct data analytics studies to review and better understand participant retention, activity and results rates.*,**,***
- Equal opportunities monitoring.*,**,***

- To report back as required to the funding bodies with which we contract – Big Lottery Fund and DWP.*,**,***

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as making your grant payment or providing activity), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our project staff).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use particularly sensitive personal information

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.

2. Where we need to carry out our legal and contractual obligations and in line with our Data Protection Policy.

3. Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our data protection policy.

4. Where it is needed to assess your capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. [We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.]

Our obligations as Minding the Gap partner organisations

We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status, to ensure your health and safety while taking part in the project and to assess your fitness to take part, to provide appropriate activity adjustments, and to monitor project absence that could lead to concern. We will also use this information to ensure meaningful equal opportunity monitoring and reporting.

- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We do not envisage that we will hold information about criminal convictions.

We will only collect information about criminal convictions if it is appropriate given the nature of the project and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the 'sign up' process or we may be notified of such information directly by you in the course of you working with us. We will use information about criminal convictions and offences in the following ways:

- To determine the most appropriate course of activity for you while on the project and where necessary to safeguard other participants/MTG employees.
- As part of the recruitment process for those working with vulnerable children and young people (DBS checks will be carried out by the appropriate partner where applicable).

We are allowed to use your personal information in this way to carry out our safeguarding children and young people obligations.

Automated decision-making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a reconsideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

We may share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

"Third parties" includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers:

- Participant referrals

- Delivery of activities in which participants can take part should they wish

- Monitoring, data tracking and audit/compliance checking (Big Lottery Fund, DWP, European Commission)

- Monitoring and evaluation (RSM/Ecorys, Big Lottery Fund, Social Enterprise East of England)

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies.

We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

When might you share my personal information with other entities in the group?

We will share your personal information with other entities in our group [as part of our regular reporting activities on project performance, in the context of project planning or a partner restructuring exercise, for system maintenance support and hosting of data, or for project evaluation/promotional activity with consent.

What about other third parties?

We may share your personal information with other third parties, for example in the context of project recruitment of new partner organisations. We may also need to share your personal information with a regulator or to otherwise comply with the law.

Data security

We have put in place measures to protect the security of your information. Details of these measures are available upon request.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Director of Business Development at Community Action Suffolk.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention

How long will you use my information for?

We will retain your information and all project information until January 2030 as required to do so by contractual arrangement with Big Lottery Fund.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

- **Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Director Business Development at Community Action Suffolk in writing.

No fee usually required

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact Director of Business Development at Community Action Suffolk. Once we have

received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact Director Business Development at Community Action Suffolk, Hannah Reid. hannah.reid@communityactionsuffolk.org.uk

I,_____ (employee/worker/contractor name), acknowledge that on _____ (date), I received a copy of [EMPLOYER]'s Privacy Notice for employees, workers and contractors and that I have read and understood it.

Signature

……

Name

……