Data Protection Impact Assessment (Trackit Lights)

Cloud computing is a method for delivering information technology (IT) services in which resources are retrieved from the Internet through web-based tools and applications, as opposed to a direct connection to a server at the school. Hurst Green Primary School operates a cloud based system. As such Hurst Green Primary School must consider the privacy implications of such a system. The Data Protection Impact Assessment is a systematic process for identifying and addressing privacy issues and considers the future consequences for privacy of a current or proposed action.

Hurst Green Primary School recognises that moving to a cloud service provider has a number of implications. Hurst Green Primary School recognises the need to have a good overview of its data information flow. The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for a cloud-based system and the impact it may have on individual privacy.

The school needs to know where the data is stored, how it can be transferred and what access possibilities the school has to its data. The location of the cloud is important to determine applicable law. The school will need to satisfy its responsibilities in determining whether the security measures the cloud provider has taken are sufficient, and that the rights of the data subject under the UK GDPR is satisfied by the school. Hurst Green Primary School aims to undertake this Data Protection Impact Assessment on an annual basis.

A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA
2. Describe the information flow
3. Identify data protection and related risks
4. Identify data protection solutions to reduce or eliminate the risks

Contents

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

What is the aim of the project? – Trackit Lights is a behaviour management system which is used in the classroom setting to motivate good behaviour and reduce administrative workload in recording performance data. Statistics are gathered across the school to provide SLT with the ability to quickly review the performance across the school.

Staff can log behaviour in a couple of clicks on any device, anywhere. Depending on the age of pupils and how the school prefer to work, it can use Trackit Lights Interactive Whiteboard app, make it more engaging for younger pupils with fun avatars, or log behaviour discreetly using a tablet or Smart Phone.

The behaviour can be sent instantly into your safeguarding system or MIS, and all other school processes are automated including behaviour analytics, house points tracking, merit certificates, email notifications, Incident Forms and Detention or Reflection Time consequences.

Trackit Lights helps teachers work 'smarter not harder' by digitising and automating all their classroom management, rewards, incident forms, detentions/reflection time, behaviour tracking, and parental engagement. Key features of Trackit Lights are as follows:

Behaviour Logging System: Teachers can log behaviour anywhere from any device

Classroom Management: Enables schools to create a positive classroom culture with the Trackit Lights Interactive Whiteboard app

Points Reward System: Class and house points are logged on the board into a school wide tracker with auto generated certificates

Monitor & Analyse Behaviour: Know what is happening in every classroom from your desk

Detention / Reflection Time: Add pupils' names to the school's centralised detention/reflection time register

Automated Incident Forms: Complete auto-populated incident forms quickly, replacing bound books and ROI Forms

Integrations (Safeguarding & MIS): Pull all the school's pupil and teacher data from its Management Information System and log behaviour straight from the board into SIMS, CPOMS and MyConcern

Parental Engagement: Parents download the Trackit Lights app from the app store and input their name and email address when logging in for the first time.

Parents are required to agree to the Trackit Lights terms and conditions which is an agreement between Trackit Lights and the parent. Trackit Lights does not receive any information about parents from the school or from Wonde. All parent data is provided by the parents.

Hurst Green Primary School uses an Application Program Interfaces (API)* which are simple, smart, and secure and gives schools more control and visibility of their own data and provides additional tools. This enables the school to link Trackit Lights to its Management Information System.

*An Application Program Interface (**API**) is a set of routines, protocols, and tools for building software applications. An **API** specifies how software components should interact.

Wonde and Third Party Apps/Vendors

Wonde's core service is used by a large percentage of schools in the UK to control the Management Information System (MIS) data it shares with third party vendors used at the school. These vendors include solutions for assessment, maths, English, library management, parent communications, parent payments, Multi Academy Trusts, voucher systems, Google/Microsoft syncing, classroom content providers etc.

Wonde is ISO27001 accredited and the majority of schools use Wonde to manage their MIS data sharing and syncing with multiple third-party vendors. An overview of how schools do

this can be found here https://www.wonde.com/school-data-management.

When a vendor (app), or vendors, requests to be connected to a school via Wonde - if the school approves that vendor(s) request and for Wonde to facilitate it, then Wonde will complete a base integration with the schools' MIS.

Wonde request (but do not extract) the permissions that are required for the majority of vendors that use its services. Wonde will then only extract and send data that has been approved by a school to send onwards to their chosen vendors. For clarity, Wonde does not extract data that is not approved by the schools for the vendors they are using.

Hurst Green Primary School can reduce the requested Wonde permissions upon the integration taking place, and Wonde can assist schools with this. Hurst Green Primary School also has the ability to change the permissions whenever it likes, but in doing so ensures that it has considered how that may affect its use of approved vendors (i.e. the flow of data to those vendors via Wonde for the vendors to provide the agreed service).

Hurst Green Primary School will undertake the following processes:

1. Collecting personal data
2. Recording and organizing personal data
3. Structuring and storing personal data
4. Copying personal data
5. Retrieving personal data
6. Deleting personal data

By opting for a cloud-based solution the school aims to achieve the following:

1. Scaleability
2. Reliability
3. Resilience
4. Delivery at a potentially lower cost
5. Supports mobile access to data securely
6. Update of documents in real time
7. Good working practice, i.e. secure access to sensitive files

The information is held securely with regular data backed up. The network is only accessible through dedicated password linked to the school.
Cloud based systems enable the school to upload documents, photos, videos, and other files to a website to share with others or to act as a backup copy. These files can then be accessed from any location or any type of device (laptop, mobile phone, tablet, etc).

The cloud service provider cannot do anything with the school's data unless they have been instructed by the school. The schools Privacy Notice will be updated especially with reference to the storing of pupil and workforce data in the cloud.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The Privacy Notices (pupil) for the school provides the lawful basis of why the school collects data. The lawful basis in order to process personal data in line with the 'lawfulness, fairness and transparency principle is as follows:

6.1 (c) Processing is necessary for compliance with a legal obligation to which the controller is subject; e.g. health & safety and safeguarding

6.1 (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.1 (f) Processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

The school has considered the lawful basis by which it processes personal data. This is recorded in Hurst Green Primary School Privacy Notice (Pupil) and where appropriate in Privacy Notice (Workforce).

How will you collect, use, store and delete data? – The information collected by the school is retained on the school's computer systems. The information is retained according to the school's Data Retention Policy.

What is the source of the data? – Pupil information is collected via registration forms when pupils join the school, pupil update forms the school issue at the start of the year, Common Transfer File (CTF) or secure file transfer from previous schools. Pupil information also includes classroom work, assessments and reports.

Will you be sharing data with anyone? – Hurst Green Primary School routinely shares pupil information with relevant staff within the school, schools that the pupil attends after leaving, the Local Authority, the Department for Education, Health Services, Learning Support Services, RM Integris and various third-party Information Society Services applications.

What types of processing identified as likely high risk are involved? – Transferring 'special category' data from the school to the cloud. Storage of personal and 'special category data in the Cloud. Some of the personal data collected may fall under the UK GDPR special category data. Trackit Lights special category data may be captured in terms of Behaviour (e.g. incidents, trends), Documents (e.g. reports, EHICs), Incidents (e.g. bullying, well-being concerns), and Indicators & related data (e.g. pupil premium, SEN).

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

What is the nature of the data? – Pupil data relates to personal identifiers and contacts (such as name, unique pupil number, contact details and address). Characteristics (such as

ethnicity, language, nationality, gender, religion, data of birth, country of birth, free school meal eligibility). Special education needs, safeguarding information, medical and administration (doctor's information, child health, dental health, allergies, medication and dietary requirements). Attendance information, assessment, attainment and behavioral information. The school also obtains data on parents/guardians/carers including their name, address, telephone number and e-mail address.

Trackit Lights collect data relating to pupil first and last names, gender, UPN, class/Year Group, FSM, SEN, Pupil Premium, and English as an Additional Language. Pupil data also includes attendance, behaviour data including incidents, comments and actions. Detention data including duration and frequency.

Workforce data includes start and end date and works e-mail address.

These are the most basic fields that are required by Trackit Lights for the system to function as intended. This data is either uploaded manually by the Trackit Lights user or is pulled from the schools MIS as verified through Wonde.

Wonde will only extract data within the scopes approved by the school. Trackit Lights define the scope of data required from the school from within Wonde. These scopes can be defined down to a granular level (i.e. first name) which is then approved by the school.

Trackit Lights is not able to access data outside of the agreed scope without further school approval.

Special Category data? – Some of the personal data collected may fall under the UK GDPR special category data. Trackit Lights special category data may be captured in terms of Behaviour (e.g. incidents, trends), Documents (e.g. reports, EHICs), Incidents (e.g. bullying, well-being concerns), and Indicators & related data (e.g. pupil premium, SEN).

The lawful basis for collecting special category information relates to Article 9 2 (g) *processing is necessary for reasons of substantial public interest and is authorised by domestic law.*

How much data is collected and used and how often? – Personal data is collected for all pupils. Additionally, personal data is also held respecting the school's workforce, Board of Governors, Volunteers, and Contractors. Data relating to sports coaches and other

educational specialist is contained within the Single Central Record to ensure health and safety and safeguarding within the school.

How long will you keep the data for? – The school will be applying appropriate data retention periods as outlined in its Data Retention Policy and the IRMS Information Management Toolkit for Schools.

Scope of data obtained? – Trackit Lights relies on minimal personal data. The school will act as the administrator and will set up access to pupils within a classroom and individual setting. Personal data will include details of the class/year and the first and second name of the pupil.

Personal data is obtained from the school's management information system. The amount of data provided to the Trackit Lights system is under full control of the school, depending on the number of features that it decides to use.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The school provides education to its students with staff delivering the National Curriculum

What is the nature of your relationship with the individuals? – Hurst Green Primary School collects and processes personal data relating to its pupils and employees to manage the parent/pupil and employment relationship.

Through the Privacy Notice (pupil/workforce) Hurst Green Primary School is committed to being transparent about how it collects and uses data and to meeting its data protection obligation. Trackit Lights is able to support the school's obligations under UK GDPR where a data subject wishes to exercise their rights.

How much control will they have? – Access to the pupil files will be controlled by the school.

Cloud Service provider is hosting the data and will not be accessing it.

The school will be able to upload personal data from its PC for the data to be stored remotely by a service provider. Any changes made to files are automatically copied across and immediately accessible from other devices the school may have.

Do they include children or other vulnerable groups? – Some of the data in Trackit Lights may have special category data such as Behaviour (e.g. incidents, trends), Documents (e.g. reports, EHICs), Incidents (e.g. bullying, well-being concerns), and Indicators & related data (e.g. pupil premium, SEN).

Are there prior concerns over this type of processing or security flaws? – Does the cloud provider store the information in an encrypted format? What is the method of file transfer? For example, the most secure way to transfer is to encrypt the data before it leaves the computer. Encryption does have its limitations since the encryption key will need to be shared with others to access the data.

Hurst Green Primary School recognises that moving to a cloud-based solution raises a number of UK General Data Protection Regulations issues as follows:

- **ISSUE:** The cloud-based solution will be storing personal data including sensitive information
  RISK: There is a risk of uncontrolled distribution of information to third parties
  MITIGATING ACTION: Trackit Lights is a 'cloud service'. Unlike conventional software which is installed onto a customer's server or PC as their own personal copy, cloud services run from a single copy of the software over the internet to which all users can log on and share.

  The service interfaces to the school's admin system via a third party service called Wonde which is used by thousands of schools and provides a secure and controlled access to specific data which the school must consent to

  Wonde, as Trackit Lights MIS integration Partner, stores school data within Amazon Web Services (AWS). The Ireland data centres are used to ensure the data stays within the EEA. Wonde are also ISO 27001 accredited. Wonde has also committed to Cyber Essentials which will follow the ISO 27001 accreditation

ISSUE: Transfer of data between the school and the cloud
RISK: Risk of compromise and unlawful access when personal data is transferred
MITIGATING ACTION: The data is encrypted. HTTPS and TLS 1.2 are both required to make a connection to Trackit Light servers. The certificate uses a signature algorithm of SHA-384 with RSA Encryption issued by Microsoft

- **ISSUE**: Security of data whilst hosted in the cloud
  RISK: Risk of compromise and unlawful access when personal data is at rest
  MITIGATING ACTION: All users have to register with their school email address and a password of their own choice. There are a very specific small number of Trackit Lights employees who have access to the system for the purposes of customer and technical support. All employees have confidentiality agreements and access is governed by individual passwords for each school

- **ISSUE:** Use of third-party sub processors?
  RISK: Non-compliance with the requirements under UK GDPR
  MITIGATING ACTION: Trackit Lights shall not use any Sub-Processor other than with the school's written permission. Tackit Lights shall inform the school of any proposed changes. It shall impose the same GDPR compliant terms on the Sub-Processor, and will be responsible to the school for the compliance of the Sub-Processor

- **ISSUE:** Understanding the cloud-based solution chosen where data processing/storage premises are shared?
  RISK: The potential of information leakage
  MITIGATING ACTION: Microsoft's UK data centres. These are government approved for use in the public sector. The location of the data centre is Scarborough North Yorkshire YO11 9HU. The data is encrypted

- **ISSUE:** Cloud solution and the geographical location of where the data is stored
  RISK: Within the EU, the physical location of the cloud is a decisive factor to determine which privacy rules apply. However, in other areas other regulations may apply which may not be Data Protection Law compliant
  MITIGATING ACTION: Microsoft's UK data centres. These are government approved for use in the public sector. The location of the data centre is Scarborough North Yorkshire YO11 9HU. The data is encrypted

  Wonde, as Trackit Lights MIS integration Partner, stores school data within Amazon Web Services (AWS). The Ireland data centres are used to ensure the data stays within the EEA. Wonde are also ISO 27001 accredited. Wonde has also committed to Cyber Essentials which will follow the ISO 27001 accreditation

- **ISSUE:** Cloud Service Provider and privacy commitments respecting personal data, i.e. the rights of data subjects
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Trackit Lights is able to support the school in its obligations with regards to a user exercising their data subject's rights, for example if they were to make a Subject Access Request (SAR) to the school acting as the data controller

  If a data subject wishes to make a Subject Access Request and/or Right to be Forgotten request, where applicable, the school can contact Trackit Lights on behalf of the requestor

- **ISSUE:** Implementing data retention effectively in the cloud
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: When a contract ends with the school, Trackit Lights take written instruction from the school on how they wish Trackit Lights to deal with their data

  The live database is deleted a month after the expiry of the contract if the school has informed Trackit Lights that they don't wish to renew their contract. The back up copies remain for one month. E-mail correspondence is retained until the end of the academic year just in case there is any follow up

- **ISSUE:** Data Back ups
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Data is hosted with cloud providers that have achieved ISO 27001. This is one of the most widely recognized, internationally accepted independent security standards. Trackit Lights data centres have earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure. This includes the management of data back ups

- **ISSUE:** Responding to a data breach
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Trackit Lights will take appropriate technical and organisational measures against the unauthorised or unlawful processing of such School Personal Data and against the accidental loss or destruction of, or damage to, such School Personal

Data to ensure a level of security appropriate to: (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (ii) the nature of the data to be protected; and take reasonable steps to ensure compliance with those measures, and notify the school's Data Controller of any data breach and the nature, details, possible consequences and mitigation actions, and submit to audit or inspection by the controller and provide further information on Trackit Light compliance as a Processor

- **ISSUE:** Subject Access Requests
  RISK: The school must be able to retrieve the data in a structured format to provide the information to the data subject
  MITIGATING ACTION: Trackit Lights is able to support the school in its obligations with regards to a user exercising their data subject's rights, for example if they were to make a Subject Access Request (SAR) to the school acting as the data controller

  If a data subject wishes to make a Subject Access Request and/or Right to be Forgotten request, where applicable, the school can contact Trackit Lights on behalf of the requestor

- **ISSUE:** Data Ownership
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: The school as data controller retains ownership of the data. Trackit Lights is the data processor

- **ISSUE:** Cloud Architecture
  RISK: The school needs to familiarise itself with the underlying technologies the cloud provider uses and the implications these technologies have on security safeguards and protection of the personal data stored in the cloud
  MITIGATING ACTION: Trackit Lights is a 'cloud service'. Unlike conventional software which is installed onto a customer's server or PC as their own personal copy, cloud

services run from a single copy of the software over the internet to which all users can log on and share.

The service interfaces to the school's admin system via a third party service called Wonde which is used by thousands of schools and provides a secure and controlled access to specific data which the school must consent to

- **ISSUE:** UK GDPR Training
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Appropriate training is undertaken by personnel that have access to Trackit Lights

- **ISSUE:** Security of Privacy
  RISK: UK GDPR non-compliance
  MITIGATING ACTION: Trackit Lights data centres are ISO27001 accredited.

  Microsoft Azure

  ISO 27001: is one of the most widely recognized, internationally accepted independent security standards. Trackit Lights data centres have earned ISO 27001 certification for the systems, applications, people, technology, processes, and data centres that make up its shared Common Infrastructure

  Wonde

  AWS computing environments are continuously audited, with certifications from accreditation bodies across the world, including ISO 27001, FedRAMP, DoD CSM, and PCI DSS. AWS is also fully compliant with applicable EU Data Protection laws, and the AWS Data Processing Agreement incorporates the Article 29 Working Party Model Clauses

  Cyber Essentials Plus certification, against which Wonde are independently audited on an annual basis. Part of this audit involves external penetration testing of our own network and systems to prove that data is held securely

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The school moving to a cloud-based solution will realise the following benefits:

- Scaleability
- Reliability
- Resilience
- Delivery at a potentially lower cost
- Supports mobile access to data securely
- Update of documents in real time
- Good working practice, i.e. secure access to sensitive files

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The views of senior leadership team and the Board of Governors will be obtained. Once reviewed the views of stakeholders will be taken into account.

The view of YourIG has also been engaged to ensure Data Protection Law compliance.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful basis for processing personal data is contained in the school's Privacy Notice (Pupil and Workforce). The Legitimate basis includes the following:

- Childcare Act 2006 (Section 40 (2)(a)
- The Education Reform Act 1988
- Further and Higher Education Act 1992,
- Education Act 1994; 1998; 2002; 2005; 2011
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law.

The cloud-based solution will enable the school to uphold the rights of the data subject? The right to be informed; the right of access; the right of rectification; the right to erasure; the right to restrict processing; the right to data portability; the right to object; and the right not to be subject to automated decision-making?

The school will continue to be compliant with its Data Protection Policy.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Data transfer; data could be compromised	Possible	Severe	Medium
Asset protection and resilience	Possible	Significant	Medium
Data Breaches	Possible	Significant	Medium
Subject Access Request	Probable	Significant	Medium
Data Retention	Probable	Significant	Medium

18

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no
Data Transfer	Secure network, end to end encryption	Reduced	Medium	Yes
Asset protection & resilience	Data Centre in UK, ISO 27001 accredited	Reduced	Medium	Yes
Data Breaches	Where applicable documented in contract and owned by school	Reduced	Low	Yes
Subject Access Request	Technical capability to satisfy data subject access request	Reduced	Low	Yes
Data Retention	Implementing school data retention periods in the cloud	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	Headteacher	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Headteacher	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Yes	DPO should advise on compliance, step 6 measures and whether processing can proceed

Summary of DPO advice:

1. Do any staff employed by Trackit receive training in regards to data protection, linked to their duty of confidentiality or have DBS clearance? Is access to customer data granted on a role / permissions-basis?
2. Are all Trackit employees aware of the company data breach procedure?
3. Do you use sub-processors? If you do use sub-processors, who are these and do they meet the same standards of data protection / GDPR as yourselves?
4. Do you use of SSL encryption and if so could you advise that standard it meets (eg. TLS 1.2 / AES-256bit)?
5. Could you advise what cloud platform you utilise and where this is located (ie. the UK)? What service ISO certifications for the hosting of data (ie. do you as a company hold ISO 27001 or is it the hosting company that holds the certification)?
6. What are the physical access controls, security of the servers, permission-based access, CCTV recording, Cyber Essentials certification, vulnerability and penetration testing?
7. Should demand unexpectedly increase, can your server hosting service scale their facilities to meet demand?
8. What resiliency does the server hosting service provide for the availability of data? Eg. mirrored data centres, how often are backups taken and how long would it take to restore from an outage? Does the service manage all security updates for the service?
9. Is Trackit data encrypted at rest on the hosting servers?
10. What is the data backup frequency?
11. How long does Trackit retain personal data for?

DPO advice accepted or overruled by Accepted

If overruled, you must explain your reasons

Comments:		
Consultation responses reviewed by: If your decision departs from individuals' views, you must explain your reasons		
Comments:		
This DPIA will kept under review by:	School Business Manager	The DPO should also review ongoing compliance with DPIA