Data Protection Impact Assessment

Blackout technologies and the Mobile Phone Policy – January 2027

Document	Data Protection Impact Assessment: Blackout technologies - education
Data controller	Kesteven and Grantham Girls' School (DFE 925/4004
Data processor	Blackout Technologies Ltd
Produced by	Elizabeth Davis, Data Protection Officer, with James Fuller, Headteacher
Version	1.0
Nest scheduled review	September 2027 or earlier on a change of supplier, function, incident or audit finding

Status key used in the tables below

	No further action required or action on track
	Action needed and due in the next quarter
	Action needed but behind target

Reviewed by governors at the Resource Management committee meeting on 29th September 2026

Using the offices and support of Blackout Technologies for IT consulting support and Keystone Law for legal insights

1. Introduction and Context

If there is a chance that a new type of processing or a new type of technology may cause a high risk to the rights and freedoms of natural persons, then it is recommended that a Data Protection Impact Assessment (DPIA) is completed by the relevant data controller.

From January 2027 Kesteven and Grantham Girls' School is introducing a revised Mobile Phone Policy, supported by Blackout Education, an application installed on students' own smartphones which restricts access to distracting applications during the school day. Because that processing involves children, operates on personal devices and is systematic in nature, the School has treated a DPIA as necessary and has completed one before the technology was brought into general use.

1.1 What is a Data Protection Impact Assessment?

Data protection impact assessments (also known as privacy impact assessments or PIAs) are a tool which will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur. The purpose of this DPIA is to systematically evaluate and mitigate the privacy and data protection risks associated with Blackout Education and aligns with the requirements of the UK GDPR, guidance from the ICO and some best practices in data security and privacy management. The primary objective is to understand the scope of data processing, identify potential risks to individuals' personal data, and implement measures that ensure legal compliance, data security, and the safeguarding of individuals' rights.

1.2 Why this processing requires an assessment

The School has screened the processing against the ICO's criteria and concludes that an assessment is required for three reasons. The processing concerns children, whose data the ICO

treats as warranting particular protection. It involves the systematic monitoring of the state of a device, albeit at a very limited level. It also takes place on equipment owned by the student or the family rather than by the School.

2. Aims of the processing, necessity and proportionality

The School operates an expectation under which mobile phones are to be switched off, out of sight and unheard on the school site. The purpose of introducing Blackout Education is to make that expectation workable in practice, to reduce the distraction that smartphones cause to learning, and to reduce the opportunity for online abuse between students during the school day.

The School has considered whether the aim could be achieved by less intrusive means. Rules alone had proved insufficient. Physical collection of handsets at the start of the day was rejected on grounds of cost, the volume of movement it would generate at the start and end of the school day, and the School's liability for a large quantity of valuable personal property. Blackout Education is more proportionate than either alternative because it processes only the state of the device, it does not read messages, browsing history, photographs, contacts or location, and it does not operate outside the scheduled school day.

Proportionality is further supported by the fact that installing the application is not the only route to compliance. Students may attend with a smartphone running Blackout Education, with a basic handset without smart functionality, or with no phone at all. A family which objects to the application is therefore not compelled to accept it, and the School will not treat a decision to use a basic handset or no handset as a disciplinary matter.

The processing covers all activity related to connecting the Mobile Phone Policy to the School's ecosystem, including the creation and maintenance of student and administrator accounts, the operation of the blocking schedule, and the reporting available to School administrators.

3. Data Categories and processing activities

The categories below are those processed by the platform. Nothing further is collected by the School through Blackout Education, and no free-text field is used to record anything about a student beyond the organisational data shown.

3.1 Administrators

Category	Data processed
Personal identifiers	Full name (first and last) and school email address
Employment data	Role within the platform, which determines the level of access held
Technical data	IP address, browser type and version, device type, login timestamps and session data

3.2 Students (on platform)

Category	Data processed
Personal identifiers	Full name (first and last) and school email address
Organisational data	Year group, form or class, and the blocking schedule that applies
Technical data	Phone make and model, operating system and version, application version, device permissions accepted or rejected, blocking status (focus mode or unrestricted), history of communications between the handset and the server, and the push token used to deliver push messages

3.3 Students (on device)

Category	Data processed
Organisational data	The blocking schedule that applies
Technical data	Phone make and model, operating system and version, application version, device permissions accepted or rejected, blocking status, and the push token

No username, password or personal data is requested or stored on the device itself.

3.4 Processing Activities

The activities comprise the ingestion of student and administrator records from the School, verification of those records, storage within a secure cloud environment hosted in appropriate data centres, processing for the purpose of identifying a device and applying the correct schedule, presentation of that information to authorised School administrators, the handling of subject access requests together with requests for rectification, erasure and restriction, and deletion in accordance with the retention schedule at section 8.

4 Lawful Basis for Processing

4.1. Legal Justifications

The school is a public authority for the purposes of section 7 of the Data Protection Act 2018 and cannot rely on legitimate interests for processing carried out in the performance of its tasks. Its lawful basis is therefore as follows:

Basis	Application to this processing
Public task, Article 6(1)(e)	The principal basis. The provision of education and the maintenance of good order and discipline are functions of a public nature conferred on the School, and the disciplinary power to regulate conduct is grounded in section 89 of the Education and Inspections Act 2006. Managing the use of mobile phones during the school day falls squarely within that function.
Legal obligation, Article 6(1)(c)	A supporting basis. The School has a duty under section 175 of the Education Act 2002, read with Keeping Children Safe in Education, to safeguard and promote the welfare of its students. Reducing the opportunity for online abuse during the school day contributes to the discharge of that duty.
Contractual necessity, Article 6(1)(b)	Relied upon by Blackout Technologies Ltd in respect of its own limited processing as a service provider, and by the School only in relation to its contract with the supplier. It is not relied upon in respect of students, who are not party to any contract with the School.

Consent is deliberately not relied upon. The imbalance of authority between a school and its students means that consent could not be freely given, and the school therefore does not present the installation of the application as a matter of consent. It does, however, offer genuine alternatives, as set out at section 2.

4.2 Data Protection Principles

Principle	How the school satisfies it
Lawful, fair and transparent	The processing rests on the bases set out at 4.1. It is fair because it is limited to the school day, because it does not extend to the content of communications, and because families are offered alternatives rather than compelled to install the application. It is transparent because the Mobile Phone Policy, explain what the application does and, equally importantly, what it does not do.
Purpose limitation	To bring personal smartphones under management in order to reduce distraction and online abuse during school periods, and to document and evaluate the effect of doing so. The data is not used for any other purpose, and in particular is not used to build a behaviour profile of an individual student or to inform decisions unrelated to the Mobile Phone Policy.
Data minimisation	Blackout requests, processes and stores only the information required to perform its function. The School provides the minimum record needed to create an account and apply the correct schedule, and does not upload additional student data.
Accuracy	As a processor, Blackout holds only the data supplied by School administrators, and the mobile applications take a snapshot of the state of the handset as accurately as the operating system permits. The School maintains accuracy by drawing account data from its management information system and by reconciling accounts at the start of each term and on any change of year group or leaving date.
Storage limitation	Storage of personal data is minimised, sensitive material such as passwords is encrypted to current good practice, and all database content and backups are held in an encrypted state in well managed data centres in the European Union. Retention is governed by section 8.
Integrity and confidentiality	The application is hosted in Amazon Web Services data centres on a three layer architecture, with regular penetration testing by reputable third parties. Development requires layered review and testing, developers do not have access to production databases, and all data is encrypted in transit and at rest. School side controls are set out at 5.1.
Accountability	This assessment, the data processing agreement with Blackout Technologies Ltd, the record of processing activities and the annual review by the Governing Board together evidence compliance.

4.3 Special category data

Blackout does not intentionally collect or process special category data such as health data or ethnicity, and the platform provides no field for it. Were a controller to enter such material into a generic free-text tag, it would be processed solely on that controller's instruction and responsibility. The school has therefore instructed administrators that no free-text field within the platform is to be used to record health, welfare, safeguarding or any other special category information, and that such matters are to be recorded only in the School's own safeguarding and pastoral systems.

5. Sub-processors

Sub-processor	Purpose	Location	Data processed and safegaurds
Amazon Web Services	Cloud hosting and infrastructure, primary	Dublin, Ireland (eu-west-1)	All data categories, held in encrypted databases. AWS Data Processing Addendum applies.
Firebase (Google LLC)	Push notifications to devices and crash reporting for application stability	EU hosted infrastructure, multiple regions	Device data comprising tokens, make and model, operating system and version, crash logs and application version. Firebase Data Processing Terms apply.
Google BigQuery (Google LLC)	Analytics on aggregated data for service improvement	EU hosted infrastructure, multiple regions	Usage statistics from which names and email addresses have been removed, but in which identifiers and device information remain. See risk R6. Google Cloud Data Processing Addendum applies.
AirByte Inc	Extract and load tool enabling secure periodic transfer from AWS to BigQuery	EU hosted, transitory only, no storage	The same reduced usage statistics as above. AirByte Trust Centre sets out its GDPR position.

The school will be notified in advance of any change to this list under the data processing agreement, and any addition will trigger a review of this assessment.

5.1. Security Controls

Control	Description
Access control	Role based access to data with multi-factor authentication. The School restricts administrator accounts to a named and minimal group, reviewed each term.
Encryption	Data is encrypted at rest and in transit.
Audit trails	Continuous logging of data access and processing activity.
Third party assurance	Regular security assessment, contractual obligation, penetration testing and compliance checking.
Staff training	Regular training on data protection, data security and breach management, extended by the School to cover the specific limits on administrator use of the platform.

6. Risks and Mitigation Strategies

The risks below record the potential effect on the rights and freedoms of individuals, taking account of both likelihood and severity and including security, privacy, compliance and reputational impacts. Likelihood is assessed as remote, possible or probable, severity as minimal, significant or severe, and overall risk as low, medium or high.

Ref	Source of risk and nature of potential impact on individuals	Likelihood	Severity	Overall risk
R1	Function creep. Administrators use the dashboard to monitor individual students beyond the purpose of the Mobile Phone Policy, or the blocking schedule is extended beyond the school day.	Possible	Significant	Medium
R2	Misunderstanding of scope. Students and parents believe the application reads messages, browsing history or location, causing distress and loss of trust even though it does not.	Probable	Significant	Medium
R3	Absence of meaningful choice. Families feel compelled to install software on a privately owned device, so that the processing is experienced as coercive.	Possible	Significant	Medium
R4	Safeguarding and welfare. A student is unable to contact home, a carer or the emergency services, or an application needed for a medical condition is blocked.	Possible	Severe	Medium
R5	Equality of access. A student without a compatible smartphone, or with a specific need, is disadvantaged or identifiable as different.	Possible	Significant	Medium
R6	Anonymised, analytics. Data transferred to BigQuery retains identifiers and device information and therefore remains personal data, although described as anonymised.	Probable	Significant	Medium
R7	International transfer. Push notification delivery and crash reporting may involve United States infrastructure.	Probable	Minimal	Low
R8	Excessive retention. Account records for leavers or former staff persist beyond need.	Possible	Significant	Medium
R9	Inaccurate account data. Records drawn from the management information system are out of date, so the wrong schedule is applied.	Possible	Minimal	Low
R10	Personal data breach at the processor or sub-processor.	Remote	Severe	Medium
R11	Supplier failure or contract termination leaving data unrecovered or undeleted.	Remote	Significant	Low

6.1 Measures to reduce risk

Each medium risk is addressed below, with the residual position and the owner responsible for the measure.

Ref	Options to reduce or eliminate risk	Effect	Residual risk	Owner and target	Status
R1	Administrator access is limited to a named group and reviewed termly. Written instructions state that the dashboard may be used only to confirm application status and to support the Mobile Phone Policy, and not for wider monitoring. Blocking schedules are configured for the school day only and are not applied in the evening, at weekends or in holidays. Access logs are reviewed each term.	Reduce	Low	Headteacher and network manager, from installation onwards	
R2	The privacy notice and the Mobile Phone Policy each state plainly what the application does and does not access. The point is made in the letter to parents.	Reduce	Low	Headteacher, before installation	
R3	Three routes to compliance are offered: a smartphone running Blackout, a basic handset, or no phone. No student is disciplined for choosing a basic handset or none, and the choice is presented neutrally. Parents may raise objections with the school, which will consider them individually.	Reduce	Low	Headteacher, HOY, in place	
R4	Calls, messaging and the emergency services remain available at all times, since the application restricts distracting applications rather than the telephone function of the handset. Applications required for a medical or accessibility need are added to the permitted list on request through the School's SEND and medical processes, and students retain the established route of contacting home through Reception.	Reduce	Low	Deputy headteacher and SENDCo, before installation	
R5	The policy is written so that having no phone is an equally acceptable position rather than an exception requiring explanation. Support is available where a family would otherwise be disadvantaged, and no list of students without smartphones is circulated.	Reduce	Low	Headteacher, Deputy headteacher, before installation	
R6	The school has recorded that this data set is pseudonymised rather than anonymous and has asked Blackout Technologies Ltd to reflect that in its documentation	Reduce	Low	Confirmation received	
R8	Accounts for leavers are deactivated at the end of the summer term and deleted in line with section 8. Administrator accounts are removed on the day a member of staff leaves.	Reduce	Low	Network Manager, termly	

	Reconciliation with the management information system takes place each term.				
R10	The data processing agreement requires notification to the School without undue delay and in any event within twenty-four hours of the processor becoming aware. The school's own breach procedure at section 10 then applies, including assessment against the seventy-two hour reporting duty.	Reduce	Low	Data Protection Officer, in place	

Risks R7, R9 and R11 are assessed as low and are accepted, subject to the safeguards described at sections 8, 9 and 4.2 respectively.

7. Individual Rights and Engagement

7.1. Transparency and Awareness

Individuals are informed of their rights through clear clear privacy notices, accessible on the school website and during onboarding.

These notices outline:

- The purpose of data processing and the new functionality brought about by introducing Blackout Education.
- Data sharing and security measures.
- Individual rights including access, rectification, erasure, restriction, and data portability.
- Contact details for data protection queries.

7.2. Personal Data Requests Handling

- Subject Access Requests: Managed jointly by Blackout Technologies and the KGGS DPO, with clear procedures for timely response. Requests can be made either through the app (automated), or via email to the data controller (school) or Blackout Technologies directly. Blackout will inform the school's DPO of any incoming requests that arrive via email.
- Rectification and Erasure: Individuals can request corrections or deletion of their data.
- Restrictions and Objections: Processes are in place to restrict processing or object based on legitimate grounds.
- Data Portability: Facilitation of data transfer to individuals upon request.

8. Data Retention and Deletion

Blackout keeps personal data only for as long as it is needed to provide the Service. Log data, 'closed' historical event data, soft-deleted items and other transitory information - which may include administrator, student or device data - are deleted within 90 days.

At the end of a contract, Blackout deletes all personal data it holds for the school: immediately where the school does not intend to export it, and otherwise once any agreed export period has passed. Retention periods and deletion schedules are reviewed periodically against our contractual obligations to schools and applicable law.

9. International Data Transfers

While core personal data remains in the EU, certain operational service components may involve transfers to the United States:

- **Firebase push notifications and crash reporting**: Firebase's service infrastructure is global. While data is stored in EU regions, the delivery of push notifications and processing of crash reports may involve Google's US-based infrastructure.
- **AWS service operations:** While data is stored in EU-West-1, AWS's control plane operations (service delivery, monitoring, and infrastructure management) are provided through AWS's global network.

9.1 Safeguards for Transfers

Appropriate safeguards protect all transfers outside the UK/EEA:

- Standard Contractual Clauses (SCCs) approved by the European Commission, implemented through:
- AWS Data Processing Addendum: https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf
- Firebase Data Processing Terms: https://firebase.google.com/terms/data-processing-terms
- EU-US Data Privacy Framework: Google LLC is certified under the Data Privacy Framework for transfers to the United States. Google's certification is available at: https://www.dataprivacyframework.gov

Technical and organisational measures:

- Both AWS and Google implement security measures, including encryption in transit and at rest, access controls, and data segregation.

10. Data Breach and Incident Management (including approach to subject access requests/GDPR complaints)

- **Breach Policy**: Established procedures for incident detection, containment, notification, and remediation shall continue to be reviewed.
- **Response Plan**: Includes internal escalation, external notification to customers and regulators, and step plan for determining if a breach has occurred.
- **Training:** Staff trained in breach identification, awareness and response.
- **Audit and Review**: Regular testing of breach response procedures.

11. Consultation and Governance

- The Client has consulted widely in the design and production of this DPIA to ensure fresh thinking, gap analysis, layered perspectives and ideas on drafting and direction of this DPIA. Consultees have included: Blackout Technologies Ltd
- Regular DPIA updates and reviews will be conducted, aligned with evolving regulations and operational changes.

12. ICO BACKSTOP & CONCLUSION

There must be a reflection before the Conclusion in any DPIA. This final step allows a gateway straight to ICO to seek help and guidance with particular risks. The Test = if residual high risk remains, you cannot proceed until you consult the ICO.

Having assessed the processing described above, the school concludes that no residual high risk remains. The risks identified are of medium severity before mitigation and reduce to low once the measures at section 6.1 are applied. Prior consultation with the Information Commissioner is therefore not required, and the processing may proceed. Should the confirmation sought under R6 not be forthcoming, or should any future change raise a risk which cannot be reduced below high, the school will consult the Commissioner before continuing.

The Headteacher is satisfied that the processing is necessary and proportionate to the aim of maintaining good order and protecting students from online harm during the school day, that it is the least intrusive of the options available, and that the safeguards described are adequate to the risk.

SIGN OFF AND COMPLETION OF THIS DPIA

Item	**Name/date**	**Notes**
DPIA produced by	James Fuller (Headteacher) and Elizabeth Davis (DPO) 22.09.26 Updated 5.10.26	
Residual risks and mitigations approved by	Resource management committee	
This DPIA will be kept under review by	Headteacher and DPO	Yearly reviews but more frequent if the need arises.