Lady Manners School

Mobile Phone Policy

Policy No:	091
Reviewed by:	DR
Approved by:	Governing Board
Minute No:	88/26
Review Cycle:	Every three years
Last Reviewed:	29 September 2026
Next Review Date:	September 2029

Through our shared school values, we aim for all students to thrive, feel included and aspire to grow as individuals who contribute to society with empathy, integrity and positivity.

This document will be reviewed 3 yearly by the Governing Board and sooner when significant changes are made to the law.

Contents

		Page
Equalities Statement of Intent		
1.	Rationale	1
2.	Aims	2
3.	Expectations	2
4.	Arrangements for Students in Years 7-11	2
5.	Arrangements for Students in the Sixth Form	3
6.	Sanctions	4
7.	About the Blackout App	4
8.	Exceptions and Accessibility	5
9.	Support and Parental Involvement	5
10.	Review and Contact	5
Appendix 1 - Blackout Information		6
Appendix 2 - DPIA		8

EQUALITIES STATEMENT OF INTENT

Lady Manners School welcomes a diverse population of both students and staff. In order to consolidate and build upon this diversity, equality of opportunity and the absence of unfair discrimination is at the core of all the school's activities. The school will not unfairly discriminate in the recruitment or general treatment of staff or students.

The school is committed to promoting and developing equality of opportunity in all its functions and will seek to do this by:

- communicating its commitment to equality and diversity to all members of the school community;
- maintaining systems for implementation, monitoring, evaluation and review;
- treating acts of discrimination and other contraventions of this policy as a disciplinary offence.

The Governing Board has responsibility for ensuring that the school operates within the legal framework for equality and for implementing the policy throughout the school. In addition, each member of the school community is responsible for preventing unfair discrimination or harassment or victimisation which it is within their control to prevent; and challenging or reporting such inappropriate behaviour if it occurs.

1. RATIONALE

We are committed to supporting the wellbeing, learning, and personal development of our students in a modern, connected world. Mobile phones are prohibited throughout the school day, including during lessons, the time between lessons, break

and lunchtime, in line with the Department for Education's statutory guidance that schools should be mobile phone-free 'by default' from 1 September 2026.

This policy is based on growing evidence, national guidance, and feedback from staff, students, and families. It provides a clear and consistent framework to ensure the appropriate use of mobile phones across all year groups.

2. AIMS

- To reduce distraction and promote focus during the school day
- To support healthy digital habits and self-regulation
- To promote fairness, consistency, and transparency across all year groups
- To balance the need for structure with family communication and safeguarding

3. EXPECTATIONS

Schools should be mobile phone-free 'by default' from 1 September 2026. Phone-free means mobile phones (and similar devices) are prohibited throughout the school day, including during lessons, the time between lessons, break and lunchtime.

Lady Manners School states the following regarding expectations:

- **All mobile phones must be in students' bags as soon as they arrive in the morning.** Any phone seen before school or during the school day on site will be confiscated.
- **At the end of the day, mobile phones are only allowed when the student leaves the school site or is on the bus bay waiting for or boarding a school bus.**
- Details for Sixth Form students differ and are explained below.

4. ARRANGEMENTS FOR STUDENTS IN YEARS 7 TO 11

Students in Years 7 to 11 must adhere to one of four approved options for mobile phone use during the school day (from when they arrive until the end of the day when they are on the bus bay or off the school site).

This approach ensures consistent expectations while giving families flexibility.

Approved Options

4.1 Smartphone with Blackout App (more information below)

- The Blackout app must be installed on a student's device by parents and will be activated during school hours.
- The app restricts access to third-party apps (e.g. social media, games, camera) but allows essential functions like:
  - Phone calls
  - SMS messages
  - Navigation (e.g. Maps)

- If the app is disabled, this will be logged on the school's centralised dashboard and visible to pastoral and administrative staff.
- The phone must still be out of sight (e.g. in a bag) throughout the day.

4.2 Basic or 'Brick' Phone

- Students may bring a simple handset that allows only calls and SMS messaging, with no/limited camera and internet function.
- The phone must still be switched off and out of sight (e.g. in a bag) throughout the day.

4.3 Hand Phone In

- Students can choose to hand their phone in each morning, switched off and collect it at the end of each day. This will be done at reception, and students may only enter one at a time.

4.4 No Phone Brought to School

- Students may leave their phone at home.

Families will confirm their chosen option with the school at the start of each academic year, with full details and permissions for the use of Blackout sent to parents and set-up support offered within the first half term.

Individual circumstances will be considered such as those who use their phone to track a medical condition.

Inappropriate use of phones will result in school sanctions being applied (details below).

Spot checks, based on families' chosen options for mobile phone expectations, will be completed throughout the year by Form Tutors and other pastoral staff.

It is important that students recognise that if the Blackout app is disabled during the school day without good reason, or the app is deleted so that a phone's status does not appear on the school's dashboard, this will result in the same sanctions as below.

5. ARRANGEMENTS FOR STUDENTS IN THE SIXTH FORM

Sixth Form students have more flexible arrangements reflecting their increased independence and responsibility.

Sixth Formers must adhere to the following:

Phones may only be used:

- In the Sixth Form Centre
- In the designated Sixth Form area in the library **ONLY** for studying purposes

Phones must be kept silent and out of sight at all other times, including:

- Corridors
- Classrooms
- The Dining Hall

Additional rules:

- Use in Sixth Form lessons is permitted only with express permission from a member of staff
- Sixth Form students must not use their mobile phones in front of younger students, and misuse of their phone will lead to the same sanctions as mentioned in section 6.

6. SANCTIONS

If a mobile phone is seen on site during the school day (this includes the bus bay in the morning), the phone will be confiscated. These sanctions also apply to when the Blackout app is disabled during the school day without good reason or a student is found to have a phone which is not what was declared at the start of the year.

First Confiscation

- The phone will be held safely at reception until the end of the day and the student will receive a 30-minute lunchtime detention.
- If the phone is confiscated at the end of the day, the phone must be handed in the following day and a detention issued.

Second Confiscation

- The phone will be held safely at reception until the end of the following day and the student will receive a 30-minute lunchtime detention.

Third Confiscation

- The phone will be held safely at reception for one week and the student will receive an after-school detention.

7. ABOUT THE BLACKOUT APP

Blackout is a mobile phone management system designed for schools, offering a trust-based approach to phone restriction. It enables students to keep their phone with them without the temptation to check their device, supporting focus and wellbeing without removing control of their devices or the function of essential apps.

What the Blackout App Does:

- Restricts access to third-party apps (e.g. social media, YouTube, games, camera) during school hours
- Allows essential functions to remain available:
    - Phone calls, SMS and iMessage, Maps/navigation
- Encourages digital self-regulation
- Displays a simple status (active/inactive) to school staff on a secure dashboard
- Can be paused manually if necessary, but this is logged for review
- Only student name and school email address is shared with Blackout as part of set-up for the app

What the App Does Not Do:

- It does not track GPS location
- It does not access, view, or store content such as messages, photos, browsing history, or files
- It does not monitor app usage, screen time, or personal data
- It does not lock the device or take remote control
- It does not share data with third parties
- It does not drain mobile data (less than 25MB per 3-month period)
- It does not drain a phone's battery; rather, it improves it due to other app restrictions

More details regarding the Blackout App are attached in the appendices, including frequently asked questions.

8. EXCEPTIONS AND ACCESSIBILITY

Allowing students with disabilities a mobile phone, where it's necessary due to the nature of their disability, may be considered a reasonable adjustment.

For students with medical conditions, a mobile phone may help them manage their medical condition - e.g. a student with diabetes might use their phone to monitor their blood sugar levels. Requests for exceptions (e.g. medical monitoring apps or accessibility features) must be made in writing to the relevant Year Leader. Each case will be reviewed individually and sensitively.

9. SUPPORT AND PARENTAL INVOLVEMENT

Parents and carers are strongly encouraged to support their child in choosing the most appropriate phone management option, to have open discussions at home about screen use, and to contact the school if they have questions or need guidance.

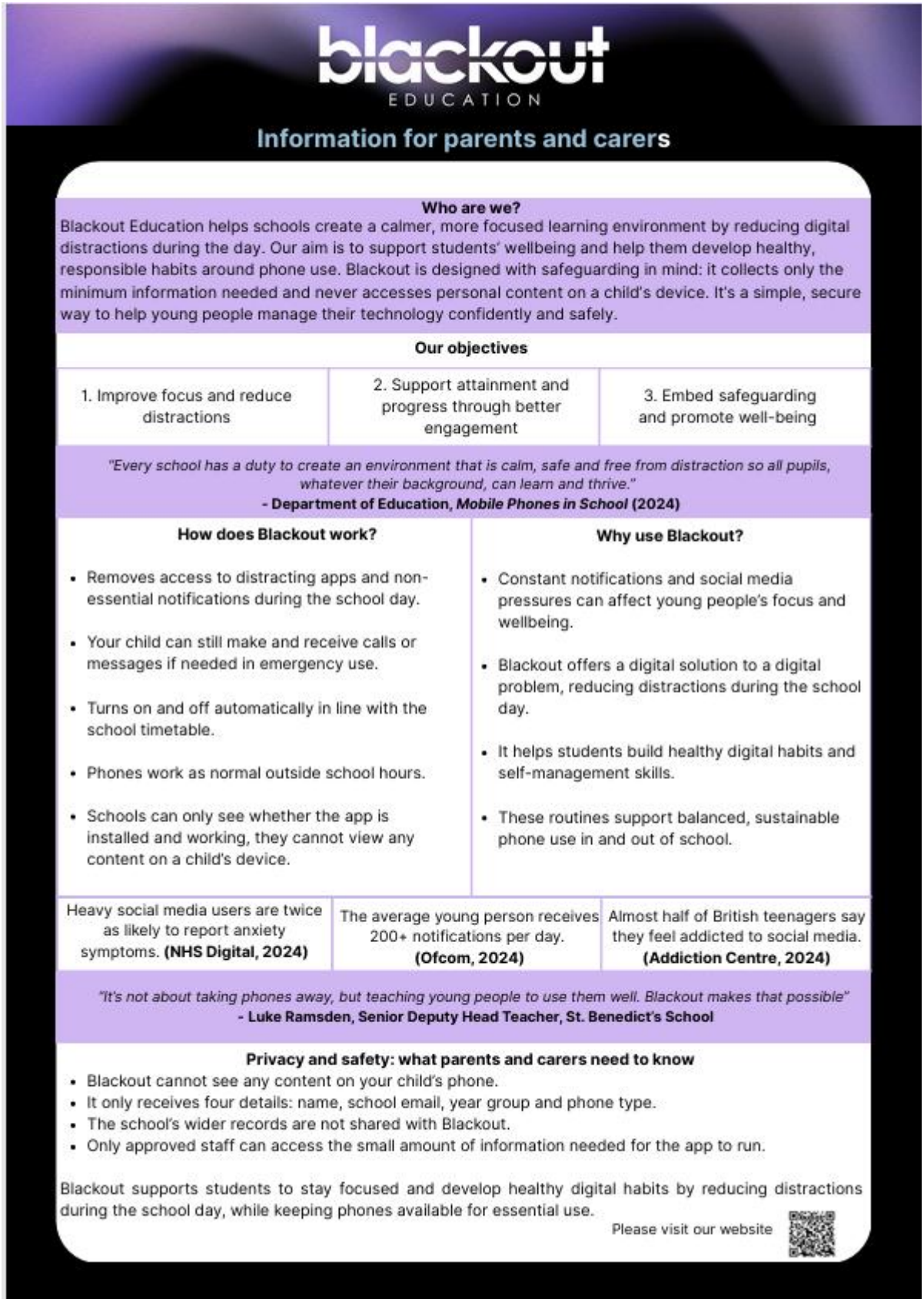
10. REVIEW AND CONTACT

This policy will be reviewed annually.
Next Review: September 2027

Appendix 1

Blackout Information including:

- Blackout Information for parents and carers
- Blackout General FAQs



blackout
EDUCATION

Information for parents and carers

Who are we?

Blackout Education helps schools create a calmer, more focused learning environment by reducing digital distractions during the day. Our aim is to support students' wellbeing and help them develop healthy, responsible habits around phone use. Blackout is designed with safeguarding in mind: it collects only the minimum information needed and never accesses personal content on a child's device. It's a simple, secure way to help young people manage their technology confidently and safely.

Our objectives

1. Improve focus and reduce distractions	2. Support attainment and progress through better engagement	3. Embed safeguarding and promote well-being

"Every school has a duty to create an environment that is calm, safe and free from distraction so all pupils, whatever their background, can learn and thrive."
- Department of Education, *Mobile Phones in School* (2024)

How does Blackout work?

- Removes access to distracting apps and non-essential notifications during the school day.
- Your child can still make and receive calls or messages if needed in emergency use.
- Turns on and off automatically in line with the school timetable.
- Phones work as normal outside school hours.
- Schools can only see whether the app is installed and working, they cannot view any content on a child's device.

Why use Blackout?

- Constant notifications and social media pressures can affect young people's focus and wellbeing.
- Blackout offers a digital solution to a digital problem, reducing distractions during the school day.
- It helps students build healthy digital habits and self-management skills.
- These routines support balanced, sustainable phone use in and out of school.

Heavy social media users are twice as likely to report anxiety symptoms. **(NHS Digital, 2024)**	The average young person receives 200+ notifications per day. **(Ofcom, 2024)**	Almost half of British teenagers say they feel addicted to social media. **(Addiction Centre, 2024)**

"It's not about taking phones away, but teaching young people to use them well. Blackout makes that possible"
- Luke Ramsden, Senior Deputy Head Teacher, St. Benedict's School

Privacy and safety: what parents and carers need to know

- Blackout cannot see any content on your child's phone.
- It only receives four details: name, school email, year group and phone type.
- The school's wider records are not shared with Blackout.
- Only approved staff can access the small amount of information needed for the app to run.

Blackout supports students to stay focused and develop healthy digital habits by reducing distractions during the school day, while keeping phones available for essential use.

Please visit our website

blackout
EDUCATION

General FAQs

What data does Blackout collect?
Only four basic details:
- Your child's name
- Their school email address
- Their year group
- Their phone type (e.g. iPhone or Samsung)

That's it.
We do not collect any data from apps, and we never access anything else on a device, such as messages, location or photos.

Can I use parental controls with Blackout?
Yes. Blackout does not block any parental controls and works alongside them, such as 'Life 360'.

What if my child leave school early or I am off sick?
Blackout can be disabled at any time by selecting a reason (for example, a medical need) and entering the unlock code. This allows you to access your device as normal when you are no longer in school.

Does Blackout track my location?
No. Blackout does not use or store your location at any time; it uses the school schedule.

Does Blackout use data or drain the device battery?
No. Blackout uses around 578KB per day – that's less than 1MB. It has almost no impact on data or battery.

For context, many popular apps use far more data each day:
- TikTok: 500-900MB
- Instagram: 300-600MB
- Snapchat: 350-700MB

Why is this data needed?
These basic details allow school staff to identify your child's device and provide support if something is not working correctly.

Many popular apps, such as Snapchat, WhatsApp and TikTok, collect much more information, including:
- Precise location
- Biometric data (such as face or voice recognition)
- Activity across other apps or websites

Blackout **does not** collect any of this data.

Who can see this information?
Your child's school's approved Blackout staff and the Blackout admin team. No one else.

What if my child needs to use a medical app (e.g. for diabetes)?
Blackout can be disabled at any time by selecting a reason, such as a medical need, and entering the unlock code. If your child relies on a medical app, we recommend speaking with the school so appropriate support can be put in place.

Can I still contact my child in case of an emergency?
Yes. Emergency calls and SMS remain available in line with the school communication policy.

Where is data stored?
All data is securely stored on AWS cloud servers in Dublin, ensuring that no data leaves the EU. Data is not sold or used for any third-party purposes.

For more FAQs, head to: https://www.blackout-technologies.com/faqs

Appendix 2

DPIA - Blackout App

DPIA – Blackout App

School Details			
Name of School	Lady Manners School		
Document Prepared by	Debbie Ridley (Deputy Head) and Jo Picknell (Deputy Head and Data Protection Lead), Data Protection Officer		
Reviewed by SLT	25/06/26		
Version History			
Version	**Date**	**Detail**	**Author**
1	2026	DPIA Created for Lady Manners	Deputy Heads and DPO

Section 1
Project Summary
When completing a DPIA, the project summary is a crucial section that helps establish an understanding of what the system, project, process or business change is about. This summary should provide sufficient information to ensure initial understanding by someone unconnected to the work

(a) Explain the Project, Process or Business Change

In order to stop smart phone use in school time, we will ask all students who intend to bring a smart phone to school to download an app which blocks access to non-essential apps during school hours. The app enables the school to block smart phone access during school hours, whilst still leaving essentials such as calls and texts functioning.

The app is called BLACKOUT and collects minimal personal data: the data subject's name and school email address.

The reasons we want to use the app are as follows:

- Reduce distraction and improve focus: The school aims to limit access to non-essential smartphone apps during the school day, helping students to stay attentive in lessons and reduce off-task behaviour and notification anxiety.

- Support attainment and progress: By reducing phone-related interruptions, the school expects greater engagement in learning, improved participation in class activities, and stronger academic outcomes.

- Embed safeguarding, wellbeing and healthy digital habits: The initiative supports wider safeguarding goals by reducing exposure to social media pressure during school hours, supporting positive digital routines, and minimising potential risks linked to online content and messaging, which will also create broader social change and positive digital habits.

- Align with national education policy and expectations: The initiative supports the government's expectations of all schools to be phone free from September 2026, whilst allowing students to keep their phones for their journeys to and from school.

- The support from the Blackout team supports the current Department for Education guidance on mobile phone use in schools, promotes behaviour standards linked to inspection expectations, and contributes to emerging priorities in the curriculum review and safeguarding reviews focused on digital literacy, online safety, personal development and student wellbeing.

(b) Proportionality

The use of this app is to stop the temptation of checking mobile phones at breaks, lunchtimes or even in lessons. Despite our previous rule (prior to the government directive) of 'off and out of sight' we continue to have issues with students using phones during the school day, some of which have caused considerable distress. This impacts student anxiety, behaviour and relationships and takes pastoral staff time away from supporting students to thrive in the school.
The app will allow all students to fully engage and raise achievement. It is also a government statutory requirement to be able to **prove** that the school day is phone free.

- **Pouches** were considered but this solution this was deemed to be too expensive; the app is fully funded. It is also possible for students to buy the de-magnetisers for the pouches online, thus making them ineffective.
- **Handing in/storing in central lockers** was also deemed too expensive, both for the storage itself and for the time that it would take to collect over 1000 students' phones each morning and return them each evening.
- **No phones in school** - this is not practical due to the long distances many of LMS students travel.

The benefits are mentioned above and include; healthier digital habits, increased engagement and improved wellbeing. Student anxiety is also reduced as students are not in fear of being filmed or receiving unwanted messages during the school day.

The app also gives the school flexibility to turn off the feature for students who need to leave school early or who are on a school trip, for example, allowing an individualised approach.

(c) Why do you need a DPIA?

The Blackout app will have access to minimal personal data of our students which is contained to the data subject's name and school email address. The app also collects the device type, class name and year group for the data subject.

Section 2

Whose Data will be collected	**Who will have access to the data collected**
• Student	• Staff who will be monitoring the dashboard this will be ICT staff, Year Leaders and SLT

Please insert a tick in the boxes below that apply. Green boxes indicate a lower risk; amber boxes indicate that the risk profile is slightly higher. Red boxes indicate 'special category' data which is a high risk. Special category data requires a lawful basis under Article 9 of the UK GDPR. The DPO will help you to identify an appropriate Article 9 lawful basis, ***but you should not process this data unless you really need to and can justify it for this project.***

Type of data	Adult	Child	Special Category Data	Adult	Child
Name	☐	þ	Sex life or sexual orientation	☐	☐
Date of Birth	☐	☐	Looked after status/ previously in care	☐	☐
Home Address	☐	☐	Health Data (Education and Health Care Plan)	☐	☐
Email Address (Work/school))	☐	þ	Race	☐	☐
Email Address (Personal)	☐	☐	Ethnic origin	☐	☐
National Curriculum year group	☐	þ	Political opinions	☐	☐
Contact telephone number	☐	☐	Religious or philosophical beliefs	☐	☐
Gender	☐	☐	Trade Union membership	☐	☐
Profiling/analytical/insights information/cookies	☐	☐	Genetic data	☐	☐
Photograph/film footage	☐	☐	Free School Meal Status*	☐	☐
Banking details	☐	☐	Student Premium Status*	☐	☐
Card payment information	☐	☐	LAC status*	☐	☐
Salary/employment benefit details	☐	☐	CIN Status*	☐	☐
Vulnerable adult data	☐	☐	Safeguarding*	☐	☐
Class name/number	☐	þ	Other: *(add any other data fields)*	☐	☐
Student UPN	☐	☐		☐	☐

*(Whilst this data is not considered special category under UKGDPR, the DFE state it would be best practice to also treat this data as Special category)

Number of individuals affected	*1200 (students in Years 7-11)*
Frequency of data transfer	*Continuous*

Section 3
Can you explain what happens to the data during the project or processing —for example how is the data collected, how it is used, where it is stored, who it is shared with and how it is deleted?

How data is collected

- **Student account details** are provided by the school (name, school email address, class group, year group).
- **Device information** is collected when the student installs the app (device type, operating system).
- **Minimal operational data** is generated during use to confirm the app is working during the school day (e.g. device status).

No data is collected from other apps, messages, photos, browsing history or content on the device.

There is no use of data for behavioural profiling, marketing, algorithmic scoring, or automated decision-making about students.

Where does the data come from?

- School MIS / student records (e.g., name, school email, year group), provided by the school.
- Students' devices - device type and installation status collected during onboarding.

- Blackout imports data via Wonde.

Will you be sharing data with anyone?

- Data is not shared with third parties for marketing or commercial gain in an identifiable form.
- Individual-level data is never shared externally and cannot be used to identify a student or their device.
- Limited access is provided to Blackout personnel only where required to support the school and maintain the service.
- The school manages access internally and can control which members of staff can view the dashboard.
- Blackout may use fully anonymised, aggregated data (for example, overall adoption levels, percentage of active devices, or year-group trends) to evaluate impact, improve the product, or communicate overall outcomes in reports or marketing materials. This data contains no personal identifiers.
- The school may also choose to use its own anonymised data to demonstrate the impact of its digital wellbeing strategy to leadership, governors or parents and carers.

When the school is informed by a parent/carer of a change of preference from Blackout, the IT team will remove the student's name, email, class, year group and device from the Blackout dashboard.

Section 4
Who is data controller and processor?

The school are data controller; Blackout is a data processor.

Section 5
What is the Lawful Basis of the processing of this data?

Public Task (Article 6(1)(e) UK GDPR)
The school is processing personal data as part of its statutory remit to:

- improve learning and attainment
- safeguard students
- uphold consistent behaviour expectations
- provide a safe learning environment

The use of Blackout supports the school's duties under:

- DfE guidance on mobile phones in schools,
- Keeping Children Safe in Education (KCSIE),
- Behaviour in Schools statutory guidance,
- Broader curriculum aims around digital literacy and online safety.

DPO Advice Note:

While Public Task (Article 6(1)(e) UK GDPR) is likely to be the most appropriate lawful basis for the school's processing of personal data in relation to the management of pupil mobile phone use, reliance on this lawful basis does not automatically mean that pupils can be required to install software on their personal devices.

Where the school offers both installation of the Blackout app and an alternative option, it should ensure that this represents a genuine choice and that both options are communicated clearly and neutrally to pupils and parents. The availability of an alternative may be relevant when demonstrating that any processing is fair and proportionate.

The school should also note that Blackout's own terms indicate that users under the age of 13 require parental consent to use the application. This parental consent relates to the child's use of the app and acceptance of the provider's terms and conditions. However, this should not be confused with the school's lawful basis under UK GDPR. The school's processing may still be undertaken under Public Task, whilst parental consent is separately obtained to meet the provider's requirements for use of the application by younger children.

Section 6
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes - The data subject's name, school email address, device type, operating system, class and year group will be disclosed to Blackout.

Section 7
How Long will the data be kept for?

- Data is retained only for the duration of the school's use of the service.
- When a student leaves the school, or when the contract ends, their account and associated device data are deleted.
- The school can request full deletion of data at any time.

Section 8
How and where will the data be stored?

- Data is stored securely in Blackout's cloud infrastructure, following standard data protection and security practices.
- Only authorised school users (ICT staff, Year Leaders and SLT) and the Schools Blackout Team can view school-level dashboards.

Section 9
Does the system or service provider have processes in place to support the exercise of individuals' rights (e.g. right of access, rectification, erasure, restriction, objection, and data portability)?

Blackout Technologies | Privacy Policy – Your Rights.

- The school remains the data controller and can:
  - request access to an individual's data
  - request correction
  - request deletion

Section 10
Does the project involve the use of new technology that may be seen as intrusive on privacy – e.g. AI, biometrics, retina scanning?

- No

Section 11
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. (Remember that information about children should be subject to higher levels of protection, as children are vulnerable data subjects. Information about children's additional learning needs, student premium status and other such information is very private information. In addition, for some children, although rare, if it were to be exposed which school they attended, this could pose a risk to their safety)

- No

Section 12
Will the project result in the school making decisions or taking action against people in a way that will significantly impact them?

The project will result in actions being taken in relation to students' use of mobile phones during the school day.
Students (with parental consent for **all** students) will be required to choose between installing the Blackout application on a personal smart device, bringing a basic phone or handing in their device in accordance with the school's behaviour policy. Compliance with the school's arrangements will be monitored and will form part of routine behaviour management processes.

The school considers these impacts to be limited and proportionate to the intended educational and safeguarding objectives, and an alternative option is available for students and their parents/carers who do not wish to install the application.

Section 13 **Who will you consult about this project?**
The school has consulted with Governors, the Data Protection Officer and information was sent to parents and carers prior to launching the app. Concerns and issues raised were responded to individually. Whilst the school is not anticipating any problems, it is proposing a staggered roll out of the app to ensure that any concerns or issues raised during the roll out are dealt with efficiently and effectively.
Additional information
Any ongoing concerns raised will be responded to by normal channels of home/school communication. Blackout Technologies | Information for guardians

Section 14 **Risks and Mitigating Actions**			
Lawfulness, fairness and transparency			
Description of risk and mitigation actions that are already in place	**Further mitigation actions that must be carried out by the school**	**Risk rating after mitigation applied**	**Person responsible**
The lawful basis for the sharing of data is [see section 5].	None	n/a	n/a
The processing is fair- sharing personal data in this way is fair (and expected).	Access to the dashboard is limited to key staff in school.	low	Deputy Head
Data subjects have a right to be informed of how their data is used. The processing will be transparent as the school will ensure that the relevant Privacy Notices are updated and/or shared.	Ensure relevant Privacy Notice(s) are updated and/or shared.	low	Deputy Head / Data Lead
Data Subjects must be able to exercise their rights under data protection laws. The rights are already available to data subjects and are explained in the school privacy notices or applicable third-party privacy notices.	Ensure that the privacy notices are up-to-date and easily available for data subjects (e.g. on school website or provided prior to processing activity)	low	Data Lead / Business services manager
Purpose limitation			
Personal data will be shared for the purpose of this processing activity. The school and provider, where applicable,	School relies on external providers documentation giving assurances	Risk reduced- keep this under	n/a

will only process personal data for the specific, agreed purpose and will not use it for any other reason beyond what is necessary to carry out that activity. The external provider has confirmed that personal data will only be used for this purpose and no other.	regarding the processing of personal data for this purpose only. Ensure personal data is only processed in line with this DPIA and that if there is 'function creep' the DPIA is revisited to address any risk.	review over time	
Data minimisation			
Personal data shared is as set out in the section 2 above. The school deems these data sets as the minimum needed for the purpose of processing.	Regularly review the data sets being processed in regard to this activity and if there are any changes ensure this is reflected in the DPIA.	Risk reduced-keep this under review over time	Deputy Head
Accuracy			
The school is responsible for ensuring personal data is accurate and up to date. All staff have a responsibility to ensure that data is factually correct.	Nominate member of staff responsible for ensuring personal data is regularly checked for accuracy. Nominate a member of staff responsible for maintaining the admin rights for the system and ensure this is known, documented and updated should any member of staff leave.	Risk reduced-keep this under review over time	MIS manager
Storage limitation			
Storage of this data is already addressed as part of school retention policies. The external provider states this data will be retained by them see section 7.	Ensure nominated staff member; • deletes data and/or requests that external provider deletes data in line with school retention requirements. • Downloads any data required to be retained upon termination of services.	Risk reduced-keep this under review over time	Data Lead
Integrity and confidentiality (security)			
Integrity and confidentiality (security) There is a risk that this processing could result in a data breach that the data controller would be responsible for. The impact of such a data breach would potentially be very high as the data relates to children who are vulnerable data subjects. Examples of risks: *Motivated intruders may try to hack the system to access personal data *Staff may accidentally share personal data with the wrong person *Personal data may be accidentally or maliciously deleted	Ensure all school staff comply with instructions and guidance regarding data protection and IT usage. Regularly train staff in data protection and cyber security. Ensure users have acknowledged the IT Security and Acceptable Use Policy Staff error is the main cause of data breaches when sharing data externally. School leadership should regularly remind and support staff to ensure that they process personal data with care and attention.	Risk reduced-keep this under review over time	Deputy Head / Data Lead

	Cyber-attacks pose a significant risk to schools. Staff should follow all cyber security guidance and instructions provided by the school and its IT provider. Key measures include: • Using strong, unique passwords and enabling multi-factor authentication where possible. • Avoiding clicking on suspicious links or opening unexpected email attachments. • Reporting any unusual activity or suspected breaches immediately. • Completing regular cyber security awareness training.		
There is a risk that the processor may not have adequate measures in place to protect personal data. The school should carry out reasonable due diligence to ensure the processor meets all required data protection standards.	Contract documentation checked. Data Sharing/Processing Agreement attached in Appendix A and reviewed against the checklist in Appendix A	Risk reduced- if documentation changes i.e., changes to the terms and conditions, this should be reviewed	Deputy Head
The minimum amount of data necessary for the purpose of the task should be used.	Ensure that data access is restricted based on user roles, so individuals can only access the information necessary to perform their specific responsibilities. Ensure users are trained in the safe use of Blackout.	Low	Deputy Head
Accountability			
There is a risk that the school may lack sufficient oversight of high-risk processing activities and may not fully understand the associated data protection risks or the measures required to mitigate them. There is a risk that the school may fail to maintain proper documentation of decisions and risk assessments.	The school, with support from the DPO, has completed the DPIA and understands all aspects of the processing activity and risks. If the responsible individual is uncertain at any stage, they should seek guidance from the DPO. This DPIA and the documents referred/linked to in this document form part of the accountability practices of the school. The DPO will ensure that all associated risks are current and will communicate any updates to schools promptly.	Low	Deputy Head

	This is a new process for the school, and the full range of risks may not yet be known. Often, risks only become apparent once the process is in operation. For this reason, this DPIA will be kept under regular review, as the understanding of risks, the use of the platform, and the way data is processed may evolve over time.		

Section 15 **Evidence of due diligence of supplier**			
As the Data Controller, the school may only rely on an external provider if it provides sufficient guarantees in relation to appropriate controls and GDPR compliance. The statements at the weblinks below have been checked by the School and the Data Protection Officer:			
External Provider Name and Address	Blackout Technologies Ltd, Capital Tower (6th Floor), 91 Waterloo Road, London, SE1 8RT		
External Provider ICO Registration Reference	ZB824847 (https://ico.org.uk/ESDWebPages/Entry/ZB824847).		
External Provider DP Contact Details	Privacy@blackout-technologies.com		
Privacy Notice	Blackout Technologies | Privacy Policyhttps://www.blackout-technologies.com/legal/website-privacy-policy		
Contract/Data Sharing Agreement	DPA_Blackout Technologies - 25 Ju		
Terms of Use	Blackout Technologies | Terms of Service		
Is there an indemnity clause relating to DP	• Yes	**If yes is the Indemnity clause reasonable?**	• Yes
Security	**Does the supplier have an incident response plan? How quickly will the supplier notify the school of a breach?** *The supplier states that it maintains an incident response process and follows a risk-based approach to breach notification in accordance with ICO guidance and reporting timelines.*		
	How and where will the data be stored? *The supplier states that personal data is stored on secure servers. Core personal data is hosted within the EU using Amazon Web Services (AWS) infrastructure located in Dublin, Ireland. The supplier also uses Google Cloud services, including Firebase, for certain operational functions.*		
	Will a restricted transfer take place? No		

	Core personal data is stored and processed within the EU (specifically on AWS cloud servers in Dublin, Ireland), ensuring it remains within European data protection borders	
	What policies do they have in place?	
	Information Security Policy **þ**	Data Protection Policy **þ**
	Privacy Policy ☑	Cyber Incident Response Plan **þ**
	Cookie Policy ☑	Play Store Privacy Policy ☑
	App Store Privacy Policy ☑	
	What Certifications and Standards do they hold?	
	Blackout Technologies are currently working towards Cyber Essentials IS020001	
	Do they offer multi factor authentication (MFA)?	
	Yes **þ** The supplier states that security controls include two-factor authentication and single sign-on options.	
	Have you enabled MFA?	
	Yes ☑	
	Does the organisation implement role-based access controls?	
	Yes **þ**	
	Is data encrypted both in transit and at rest?	**Yes**

Appendix A - Checklist for Data Processing Agreements		
A Data Processing Agreement must set out:	**Document Name (see appendix A)**	**paragraph/ clause number**
1. The subject-matter of the processing	Data Protection Agreement	2
2. How long the processing will continue for	Data Protection Agreement	Annex 1
3. The nature and purpose of the processing	Data Protection Agreement	Annex 1
4. The type of personal data	Data Protection Agreement	Annex 1
5. The categories of data subject	Data Protection Agreement	Annex 1
6. The controller's obligations and rights	Data Protection Agreement	4.13
Processor Obligations		
7. The processor will only process the personal data in accordance with our written instructions, unless required to do so by law	Data Protection Agreement	

8. The processor must obtain a commitment of confidentiality from anyone it allows to process the personal data, including staff, agency workers and volunteers.	Data Protection Agreement	6
9. The processor must put in place appropriate technical and organisational measures to ensure the security of any data they process	Data Protection Agreement	7 and Annex 3
10. The processor must assist the controller and also to take "appropriate technical and organisational measures" to help the controller respond to requests from individuals to exercise their rights.	Data Protection Agreement	9
11. The processor will notify the controller of any personal data breach without undue delay	Data Protection Agreement	8.30
12. To assist with any Data Protection Impact Assessment	Data Protection Agreement	10
13. The processor to provide the controller with all the information that is needed to show that the obligations of Article 28 have been met; and	Data Protection Agreement	
14. The processor to allow for, and contribute to, audits and inspections carried out by the controller, or by an auditor appointed by the controller.	Data Protection Agreement	12
At the end of the contract the processor must:		
15. at the controller's choice, delete or return to the controller all the personal data it has been processing for it; and	Data Protection Agreement	11
16. delete existing copies of the personal data unless EU or Member State law requires it to be stored.	Data Protection Agreement	11
Using sub-processors:		
17. The Processor must not use another processor (a sub-processor) without the controller's specific or general written authorisation	Data Protection Agreement	5.19
18. If a sub-processor is engaged, there must be a contract in place which gives effect to terms substantially similar to the one between the controller and processor	Data Protection Agreement	5.21
19. if a sub-processor is employed under the controller's general written authorisation, the processor should let the controller know of any intended changes and give the controller a chance to object to them	Data Protection Agreement	5.20
20. The processor is liable to the controller for the sub-processor's compliance with its data protection obligations	Data Protection Agreement	5.22
Section 16 **Risk rating Decision**		
As a result of the privacy risks and mitigations it has been evaluated that the overall level of residual risk to privacy after the mitigation actions have been carried is medium. The school leadership and governance should note this risk and if appropriate, include it in the Information Risks section of the School/Trust Risk Register.		
Section 17 **DPO Advice & School Sign Off**		
Based on the information available at the time of writing and the checks made on the provider's documentation the DPO is satisfied that this DPIA addresses the main data protection risks of processing personal data in this way. **The DPO will update this DPIA when notified of relevant changes or upon becoming aware of them. If the school receives any updates or identifies new risks associated with this project, please notify the DPO as soon as possible.**		

Summary of DPO advice:

- Ensure the measures identified in the risk mitigation table are actioned
- Ensure the DPIA is approved according to your Data Protection Policy and internal processes
- Add this DPIA to your ROPA (Record of Processing Activities)
- Add this processing to your privacy notice if appropriate
- Ensure the lawful basis and justification for using the Blackout app are clearly documented, including why the solution is considered necessary and proportionate and why any less intrusive alternatives were not considered sufficient.
- Ensure any alternative options available to pupils (for example, handing mobile phones in) are presented as a genuine choice and communicated clearly and neutrally to pupils and parents.
- Remove references to Blackout being the "recommended" option if the school intends to offer alternative arrangements, as this may undermine evidence of a genuine choice.
- Consult with pupils and parents before implementation and document the outcome of that consultation within the DPIA and decision-making process.
- Develop and document a clear operational procedure covering how the arrangement will be managed in practice, including monitoring arrangements, staff responsibilities, escalation processes and arrangements for pupils who choose not to install the app.
- Consider governor review and approval prior to implementation to provide appropriate oversight, challenge and an audit trail demonstrating that risks have been considered at an appropriate level.
- Do not commence processing until the DPIA has been completed, outstanding actions addressed, and appropriate approvals obtained.
- Keep this document under review; if there are changes to the way personal data is processed, review the DPIA, make any necessary amendments and save as a new version.

Reviewed by DPO:	Alex Steward, DPO, Education Data Hub.
Date of DPO review:	24/09/26
Date of internal review:	24/09/26
DPO advice accepted or overruled by:	Lady Manners School Deputy Head and Data protection Lead
Decision	☑ The school **will** proceed with the project, process or business change.
This DPIA will be kept under review by:	Debbie Ridley