BRINGING YOUR OWN DEVICE (BYOD) STUDENT POLICY

Policy implemented:	September 2025
Last reviewed:	September 2026
Next review due:	September 2027

EQUALITY AND DIVERSITY STATEMENT

Salutem Care & Education is committed to the fair and equitable treatment of all individuals in accordance with the Equality Act 2010. An Equality Impact Assessment has been completed for this policy to ensure it can be applied consistently and without discrimination. Salutem Care & Education is committed to safe, high-quality, person-centred services that uphold people's rights and dignity.

All colleagues (including volunteers, agency workers and contractors) must follow this policy, guided by our values. Policies are reviewed every two years; if a review is delayed, the current version remains in force until approved by the Policy Sponsor.

Training will support understanding, and people we support will be involved in reviews. Local procedures may support this policy, but corporate policies must not be changed locally without formal approval.

This policy must be shared with all colleagues. The controlled version is on BLINK; printed/downloaded copies may be out of date

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

1. Summary

This policy sets out the requirements for students who bring personal devices onto Beaumont College premises and connect to the Beaumont College student wireless network ("Beau Devices"). The policy supports the safe, secure and appropriate use of personal technology for learning, communication and independent living whilst ensuring compliance with safeguarding, data protection and information security requirements.

The policy applies equally to students attending educational provision and those accessing residential services.

2. Document Control

Policy Sponsor (Name & Role):	Natalie Forsythe (Lead Assistive Technologist)
Policy Reviewer (Name & Role):	Vicky Muncaster (Assistant Principal)
Approved by (Name/Role):	Aaron Churchyard (Quality Manager)
Date Implemented:	September 2025
Last Reviewed:	September 2026
Next Review Due:	September 2027
Version Number:	V2.0
Controlled Copy Location:	☐ BLINK ☒ Education Policy Hub
Policy category (tick):	☐Safeguarding ☐ Health & Safety ☐ Care practice ☐ HR/People ☒ Education ☐ Information Governance ☐ Other: [ ]

Policy Applies to:	**People we Support** ☐ Children/young people ☐ Adults ☒ Learners **Workforce** ☒ Permanent ☒ Bank ☒ Agency ☐ Other: [ ]	☐ Families/Carers ☐ Volunteers ☐ Contractors

Contents

1. Summary....2
2. Document Control....2
3. Contents....3
4. Definitions....4
5. Principles....4
6. Monitoring, Audit and Compliance....9
7. Areas of Responsibility....9
8. Learning and Development....10
9. Associated Documents....11
10. Legal, Regulatory & Standards Framework....11
11. Version Control....11
12. Appendices....12

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

4. Definitions

BYOD
Bring Your Own Device. Personal devices owned by a student including smartphones, tablets, laptops and similar technology.

Beau Devices
Beaumont College's student Wi-Fi network.

DSL
Designated Safeguarding Lead.

AUP
Acceptable Use Policy.

Web 2.0 Risk Assessment
Assessment completed to determine suitable access to online services and internet-based platforms.

Monitoring Certificate
A security certificate installed on a device to enable filtering, monitoring and protection whilst connected to the college network.

Principles

5.1 Purpose and Scope
Beaumont College recognises that personal devices can play a valuable role in supporting learning, communication, independence and access to information. This policy establishes the expectations and requirements for students who bring personal devices onto college premises or access the college's wireless network. The policy applies to all students accessing educational and residential provision and covers educational, communication and personal use of devices whilst connected to college systems or networks.

This policy should be read alongside the College Safeguarding and Child Protection Policy, the Acceptable Use Policy, the Prevent Policy, the Equality and Diversity Policy and other associated safeguarding and information governance procedures. Any safeguarding concerns arising from device use must be reported immediately to the Designated Safeguarding Lead (DSL) and managed in accordance with safeguarding procedures.

In this policy, "the Organisation" means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to "Salutem" are used as a short form.

5.2 Standards of Practice

5.2.1 Use of Personal Devices

Students may bring personal devices onto college premises and into residential provision where their use supports learning, communication, independence and personal wellbeing. Personal devices may be used to access educational resources, undertake research, participate in learning activities, take notes and utilise approved educational applications. During breaks, social times and within residential settings, devices may also be used for personal and leisure activities, provided such use remains appropriate and does not negatively impact the learning environment or the safety and wellbeing of others.

5.2.2 Respectful and Appropriate Use

All students are expected to use personal devices responsibly, respectfully and in a manner that reflects the values of the college community. Device use must not disrupt learning activities, interfere with the experience of other students, or compromise the safety, dignity or wellbeing of any individual. The use of personal devices for cyberbullying, harassment, discriminatory behaviour, sharing inappropriate material, participating in harmful online activities or engaging in unsafe online interactions is strictly prohibited and may result in safeguarding intervention and disciplinary action.

5.2.3 Photography, Audio and Video Recording

Students must respect the privacy and rights of others when using cameras, audio recording functions or video recording facilities on personal devices. Photographs, audio recordings or video recordings must not be taken without the explicit consent of those involved. Unauthorised recording of students, staff, visitors or college activities is prohibited and may be investigated as a safeguarding or disciplinary concern.

5.3 Network Access and Internet Safety

5.3.1 Access Requirements

Access to the Beau Devices wireless network is subject to students having completed the relevant Acceptable Use Policy and any required Web 2.0 Risk Assessment. The college may implement

additional controls or requirements where necessary to ensure the safety of students and the security of college systems. Guest access may be provided in limited circumstances and will be subject to appropriate restrictions.

5.3.2 Filtering and Monitoring

As part of its safeguarding and information security responsibilities, the college reserves the right to monitor and filter internet activity undertaken through its network. Monitoring is undertaken to protect students from harmful content, support safeguarding responsibilities, maintain network security and ensure compliance with college policies. Monitoring arrangements are proportionate, lawful and focused solely on activity taking place through the college network.

5.3.3 Installation of Security Certificates

To support filtering, monitoring and cyber security measures, the college may require the installation of monitoring and filtering certificates on personal devices as a condition of network access. These certificates enable the college to identify inappropriate or harmful online activity and maintain a safe digital learning environment. The installation of these certificates does not provide access to personal content stored on the device, including photographs, messages or locally stored files. The AT/IT Team will provide support with installation and compatibility where required.

5.4 Accessibility and Inclusion

The college is committed to ensuring that all students can access digital learning opportunities regardless of their personal circumstances. Where a student does not have access to a suitable personal device, reasonable efforts will be made to provide alternative equipment or loan devices. Students may also be supported through the provision of training, guidance and reasonable adjustments that promote safe and effective engagement with technology.

5.5 Risk Assessment and Management

5.5.1 Device Security

Students are responsible for maintaining the security of their personal devices and should take appropriate steps to protect their information and prevent unauthorised access. Devices should be secured through the use of passwords, PINs or similar security measures and should be kept up to date with the latest operating system and security updates. Students are encouraged to install appropriate antivirus protection and promptly report any concerns relating to device security.

In this policy, “the Organisation” means Salutem Care & Education [Salutem Ld Bidco Iv Limited, Pathways Care Group Limited, Pathways 4 Care Ltd, Modus Care Limited, Clearwater Care (Hackney) Limited, Greenfield Close Residential Home Limited, Salutem Shared Services Limited, Salutem Shared Services Ii Limited, Salutem Shared Services Iii Limited, Modus Care (Plymouth) Limited, Salutem Ld Bidco Limited, Salutem Ld Bidco Ii Limited, Salutem Ld Topco Limited, Salutem Ld Topco Ii Limited, Newlife Care Services Limited, Pathways Daycare Limited, Amity Residential Care Limited]. References to “Salutem” are used as a short form.

5.5.2 Safe Charging and Usage

Personal devices must be used and charged safely at all times. Students are expected to follow college health and safety guidance, including the use of designated charging points where available and avoiding unsafe charging practices that may create a fire risk. Devices should be used in accordance with staff instructions and in a manner that does not present a risk to the user or others.

5.5.3 Bandwidth Management

The college retains the right to manage network capacity and restrict access to websites, applications or services where necessary. Such restrictions may be introduced to maintain network performance, support safeguarding obligations, prioritise educational use and prevent misuse of college systems.

5.6 Safeguarding and Escalation

The safety and wellbeing of students remain the college's primary consideration when personal devices are used on site or connected to college systems. Staff are expected to remain vigilant to potential online safeguarding risks, including cyberbullying, exploitation, radicalisation, grooming and exposure to harmful content. Any concern identified through observation, disclosure or monitoring activity must be recorded and reported to the DSL without delay. Where safeguarding concerns are identified, appropriate action will be taken in line with safeguarding procedures, including engagement with parents, carers and external agencies where necessary.

5.7 Recording and Reporting

Students are expected to report concerns relating to personal device security, misuse of the network, loss or theft of devices, or online safety concerns as soon as reasonably possible. Reports may be made to teaching staff, residential staff, the AT/IT Team or a member of the safeguarding team. All safeguarding concerns relating to device use will be recorded and managed in accordance with college safeguarding procedures.

5.8 Confidentiality and Data Handling

5.8.1 Data Protection

The college will process any information obtained through network filtering and monitoring in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and organisational information governance requirements. Information will only be collected where necessary for safeguarding, security or operational purposes and will only be accessible to authorised personnel. Data will be retained and disposed of in accordance with established retention schedules.

5.8.2 Privacy

The college is committed to balancing student privacy rights with its responsibilities to protect students and maintain a secure learning environment. Monitoring activities are proportionate and limited to internet activity undertaken whilst connected to the college network. Students will be informed of the purpose of monitoring activities and how their information may be used.

5.9 Restrictions on Device Use

Students must not use personal devices to access illegal, harmful, violent, extremist, gambling or otherwise inappropriate content. Attempts to bypass network controls, compromise college systems or install unauthorised software that could affect network security are strictly prohibited. Additional restrictions may apply to students under the age of 18 in accordance with safeguarding and legislative requirements.

5.10 Student Responsibilities

Students are responsible for ensuring that their use of personal devices complies with this policy and all associated college procedures. They must take reasonable steps to protect their devices, follow staff instructions regarding device use, report concerns promptly and use personal technology in a manner that supports a safe and positive college environment. Students remain responsible for the care and security of their own devices, and the college accepts no liability for loss, theft or damage. Students are therefore encouraged to consider appropriate insurance arrangements.

5.11 Disciplinary Action

Failure to comply with this policy may result in restrictions being placed on device or network use, temporary suspension of wireless access, confiscation of devices where appropriate for

investigation purposes, or formal disciplinary action under the relevant college procedures. Where concerns also constitute a safeguarding matter, safeguarding processes will run alongside any disciplinary investigation. Serious breaches may be referred to external agencies, including the police.

6. Monitoring, Audit and Compliance

6.1 Compliance Monitoring

The college will monitor compliance with this policy through routine safeguarding oversight, review of reported incidents, network monitoring activity, quality assurance processes and management review. Monitoring arrangements are designed to provide assurance that students are using devices and network services appropriately and that safeguarding and information security controls remain effective.

6.2 Reporting Arrangements

Information relating to compliance, safeguarding concerns and significant incidents will be reported through established governance arrangements. Relevant information may be reviewed by operational leaders, safeguarding leads, quality assurance teams and senior leaders to ensure the effectiveness of policy implementation and identify any required improvements.

6.3 Managing Non-Compliance

Where non-compliance is identified, the college will seek to promote understanding and improve compliance through support, education and guidance wherever appropriate. Where behaviours continue or present an increased risk to individuals, systems or the organisation, additional restrictions, disciplinary action or safeguarding interventions may be implemented.

7. Areas of Responsibility

7.1 Divisional Senior Leadership Team

The Senior Leadership Team is responsible for ensuring that appropriate governance arrangements are in place to support the safe and effective use of personal devices across the college. This includes ensuring compliance with relevant legislation, safeguarding requirements and

organisational standards, whilst promoting a culture of digital safety and responsible technology use.

7.2 Beaumont College Education Leadership

Education leaders are responsible for implementing this policy within their areas of responsibility and ensuring that students understand the expectations placed upon them. Leaders will monitor compliance, respond to emerging concerns and ensure that staff are appropriately supported in applying the requirements of the policy consistently.

7.3 Designated Safeguarding Lead

The Designated Safeguarding Lead is responsible for responding to safeguarding concerns arising from the use of personal devices, ensuring appropriate records are maintained and determining whether concerns require escalation. The DSL will monitor patterns and trends to identify emerging online safety risks and ensure appropriate safeguarding responses are implemented.

7.4 AT/IT Team

The AT/IT Team is responsible for administering network access arrangements, maintaining filtering and monitoring systems and supporting the installation of monitoring certificates where required. The team will also provide appropriate technical support and work collaboratively with safeguarding and operational colleagues to maintain network security.

7.5 Students

Students are responsible for complying with the requirements of this policy, using personal devices appropriately and cooperating with safeguarding, security and information governance measures. Students are expected to contribute positively to a safe, respectful and inclusive digital environment for all members of the college community.

8. Learning and Development

8.1 Student Awareness

Students will receive guidance regarding:

- Safe use of personal devices.
- Online safety and safeguarding.
- Acceptable use requirements.
- Reporting concerns.

8.2 Staff Training

Staff responsible for implementing this policy will receive training appropriate to their role, including safeguarding, online safety and information governance awareness.

9. Associated Documents

- Safeguarding and Child Protection Policy
- Acceptable Use Policy (Supported and Independent Versions)
- Web 2.0 Risk Assessment Process
- Prevent Policy
- Equality and Diversity Policy
- Behaviour and Disciplinary Policy
- Data Protection and Information Governance Policies
- Beaumont College Intake Policy

10. Legal, Regulatory & Standards Framework

- Data Protection Act 2018
- UK GDPR
- Equality Act 2010
- Education Act 2002
- Keeping Children Safe in Education (KCSIE)
- Working Together to Safeguard Children
- Prevent Duty Guidance
- Relevant Ofsted Requirements
- Salutem Policies and Governance Standards

11. Version Control

This is a controlled document. As a controlled document, any printed copies of this document, or saved onto local or network drives should be actively monitored to ensure the latest version is always available.

Version Number	Date	Author	Summary of Changes	Approved By
V1.0	September 2025	Natalie Forsythe	New policy	Craig Harris
V2.0	September 2026	Natalie Forsythe	Policy migrated to the Salutem policy format and language standard with no material change to the policy intent or requirements.	Aaron Churchyard
V2.1	September 2026	Vicky Muncaster	Reviewed	

12. Appendices

- Appendix A: (e.g., checklist)
- Appendix B: (e.g., flowchart)