Bring Your Own Device (BYOD) Policy

Halton SEND Parent Carer's Forum

Your voice counts

Policy owner	**Steering Group**
Approved on	4 November 2026
Next review	4 November 2027
Version	1.0 – approved
Signed by / Authorised by	Clare Collins, Chairperson

Contact: info@haltonsendpcf.org.uk | haltonsendcarersforum.org.uk

Postal address: Office 2, 2 Linacre Lane, Widnes, Cheshire, WA8 9DN

This policy is adapted from the supplied BYOD draft for the Forum's community engagement, co-production and SEND parent carer participation activities.

Contents

- 1. Purpose
- 2. What this policy covers
- 3. Who the policy applies to
- 4. Basic security expectations
- 5. Protecting personal information
- 6. Messaging, email, apps and online services
- 7. Photographs, videos and recordings
- 8. Loss, theft, suspected compromise or data breach
- 9. Leaving the Forum or changing role
- 10. Personal use and privacy
- 11. Costs and equipment
- 12. Children, young people and adults at risk
- 13. Responsibilities of the Forum and users
- 14. Acknowledgement

1. Purpose

Halton SEND Parent Carer's Forum (the Forum) recognises that staff, steering group members, parent carer representatives and volunteers may use their own phones, tablets and computers to support Forum activities, engage with families and partners, attend meetings and produce information.

This policy sets practical and proportionate expectations to protect parent carers, children and young people, Forum information, devices and the Forum's reputation. It supports inclusive participation while recognising that access and security arrangements may differ according to a person's role and the information they handle.

2. What this policy covers

A personal device is a phone, tablet, laptop or computer owned or primarily used by an individual but used for Forum business. Activities may include:

- Using authorised Forum email, messaging, social media or online meeting accounts.
- Accessing Forum documents, consultation responses, surveys, cloud storage, minutes or meeting papers.
- Preparing newsletters, event materials, reports and co-production documents.
- Taking photographs, videos or recordings at Forum activities when authorised.
- Communicating with parent carers, volunteers, practitioners or partner organisations.

3. Who the policy applies to

This policy applies to anyone authorised to use a personal device for Forum activity, including staff, the Steering Group, volunteers and parent carer representatives. Authorisation and access should reflect the person's actual role.

The Forum should offer reasonable alternatives where practical to anyone who cannot or does not wish to use their own device. Using a device does not, in itself, change anyone's employment or volunteer status.

4. Basic security expectations

Anyone using a personal device for Forum work must take reasonable steps to protect it and the information accessed through it:

- Use a PIN, password, biometric lock or other secure screen lock; lock the device when unattended.
- Keep operating systems, apps and security protections updated, and avoid knowingly compromised software.
- Use unique account passwords; never share credentials. Enable multi-factor authentication where available and practical.
- Do not allow others, including family members, to use an unlocked device while Forum data or accounts are accessible. Forum email must not be accessed from shared or family devices.
- Avoid saving Forum documents in personal photo libraries, downloads folders, unapproved cloud backups or unsecured USB drives.
- Do not use insecure public Wi-Fi to view sensitive Forum information unless appropriate protections are in place.
- Report concerns promptly rather than attempting to conceal a mistake.

5. Protecting personal information

Personal information must be handled in accordance with the UK GDPR, the Data Protection Act 2018 and the Forum's information governance arrangements. SEND-related information can be especially sensitive, including details of a child's health, disability, education, support needs and family circumstances.

- Only access, collect or retain personal data needed for an agreed Forum purpose.
- Use approved Forum systems and storage for parent carer contacts, surveys, consultations, case examples and meeting records.
- Do not download membership lists or bulk parent carer data to personal devices, USB drives or personal cloud accounts.

- Avoid recording identifiable information about children or families in personal notes, personal messaging apps or personal email.
- Use anonymised or appropriately consented examples when contributing to co-production, reports or partner discussions.
- Check recipients and attachments before sending. Use BCC when contacting groups whose email addresses should not be shared.
- Follow agreed retention and secure deletion arrangements; do not retain personal copies once no longer required.

6. Messaging, email, apps and online services

Use Forum-approved email accounts, messaging channels, collaboration tools and cloud services for Forum business wherever available. Access must be authorised and limited to those who need it.

- Do not forward confidential Forum emails or attachments to personal accounts unnecessarily.
- Do not add parent carers, staff or partners to group chats without an appropriate reason and any necessary consent.
- Do not post identifying family information, screenshots, private correspondence or sensitive meeting content to social media or informal groups.
- Agree who administers shared accounts, grants and removes access, keeps essential records and manages backups.
- Use approved meeting links and account settings for virtual meetings; check privacy settings and attendees before sharing sensitive information.

7. Photographs, videos and recordings

Photographs, video, audio and screenshots may be useful for Forum events, promotion and participation, but must be handled carefully. Before recording or sharing, consider the purpose, notice to participants, lawful basis or consent, people who may need additional protection, access and storage arrangements.

- Follow the Forum's photography, communications and safeguarding procedures.
- Do not photograph or record children, young people or participants who have not been appropriately informed or where required permission is absent.
- Do not publish images or names of children, families or attendees without appropriate authorisation.
- Transfer approved event media promptly into Forum-controlled storage and remove unnecessary personal-device copies.
- Do not make unauthorised recordings of confidential meetings, discussions or personal disclosures.

8. Loss, theft, suspected compromise or data breach

Immediately notify the Forum's designated contact if a device is lost or stolen, accounts may have been accessed improperly, information is sent to the wrong person, or a data breach is suspected. Report even if the facts are not yet fully known.

Data protection / incident contact: [Insert named role and contact details]

The Forum will assess the situation promptly, document it and decide what action is needed, including account restriction, password changes, recovery or deletion where lawfully and technically possible, advice to affected individuals and any required regulatory reporting. The Forum, not the individual user acting alone, will assess applicable breach-reporting duties and deadlines.

People should report mistakes quickly without fear of automatic blame. The priority is to limit harm and protect families and Forum information.

9. Leaving the Forum or changing role

When a staff member, steering group member, parent carer representative or volunteer leaves or changes responsibilities, they must stop using any access that is no longer authorised, transfer Forum records to approved storage, remove unnecessary local and personal-cloud copies and report any remaining access.

The Forum should promptly review and remove account permissions, shared links and administrative access as appropriate.

10. Personal use and privacy

A personal device remains the property of its owner. The Forum will not normally inspect or control private devices or personal messages, photographs, contacts and files. Any request concerning Forum information on a personal device must have a genuine, lawful and proportionate reason and be handled sensitively.

11. Costs and equipment

Unless separately agreed, individuals remain responsible for normal personal mobile, data, broadband and equipment costs. The Forum should consider reasonable alternatives or agreed reimbursement where needed for equitable participation. No volunteer should be required to incur significant costs without prior agreement.

12. Children, young people and adults at risk

The Forum engages with families of children and young people with special educational needs and disabilities. Personal-device use must never bypass the Forum's safeguarding procedures or create inappropriate direct contact with children and young people.

- Use approved contact arrangements and keep boundaries clear for direct messages and online participation.
- Keep identifiable safeguarding information secure and share only with authorised people who need to know.
- Report safeguarding concerns arising from messages, photographs, recordings, online behaviour or data handling using the Forum safeguarding procedure.

Safeguarding contact: [Insert named role and contact details]

13. Responsibilities of the Forum and users

The Forum, within available resources, will identify approved accounts, provide proportionate guidance, restrict access by role, respond to incidents, support staff and volunteers and review this policy at least annually or sooner if circumstances change.

All authorised users are responsible for following these requirements, seeking advice if unsure, respecting confidentiality and reporting risks promptly. The Steering Group retains oversight of this policy and any subsequent revisions.

14. Acknowledgement

I confirm that I have read and understood the Halton SEND Parent Carer's Forum Bring Your Own Device Policy and agree to take reasonable steps to safeguard information I access or hold on the Forum's behalf.

Name: _____

Role: _____

Signature (if required): _____

Date: _____

Approved by / Authorised by: Clare Collins, Chairperson

Approval date: 4 November 2026 Next review: 4 November 2027