

# May Blossom Farm CIC

## Alternative Provision

Registered Office: 30 Bath Street, Rugby, Warwickshire

Phone: 07870 853725

Email: [info@mayblossomfarm.co.uk](mailto:info@mayblossomfarm.co.uk)

Web Site: <http://www.mayblossomfarm.co.uk>



# Online Safety Policy

<b>Approved by:</b>	Gill Press
<b>Last reviewed on:</b>	01/09/2025
<b>Next review due by:</b>	31/08/2026
<b>Head of Alternative Provision</b>	Gill Press
<b>Deputy Head of Alternative Provision</b>	Hannah Priest
<b>Designated Safeguarding Lead (DSL)</b>	Gill Press
<b>Deputy DSL (DDSL)</b>	Hannah Priest
<b>Designated Safeguarding Trustee</b>	Russel Breyer

This policy was ratified in Sept 2025 and will be reviewed in September 2026

## 1. Purpose

This policy outlines the acceptable use of ICT systems, devices, internet access, and digital communication tools at May Blossom Farm. It applies to all students, staff, and visitors who use our ICT resources. The aim is to promote the safe, responsible and lawful use of technology, protecting users from harm and ensuring compliance with statutory safeguarding responsibilities under **Keeping Children Safe in Education**.

May Blossom Farm CIC AP is a small organisation, in its start-up phase, with very high ratios of staff to students. During this start-up period, we are using a combination of DNS filtering to block access to harmful or inappropriate online websites and content from any student device used at May Blossom Farm, together with close staff real-time supervision – with a sightline to screens - of student use of May Blossom Farm ipads, combined with after the event monitoring of browsing history and device use. As our financial situation allows, we will move to supplementing these approaches with Lightspeed DNS filtering software on all student May Blossom Farm devices.

The May Blossom Farm network separates staff access from student access to the internet. Staff and students have separate Virtual Local Area Networks (VLANS) which are not interconnected.

Staff are expected to conform to professional standards, set out clearly in this and other policies.

May Blossom Farm student devices currently comprise 2 ipads. Staff devices currently comprise one laptop and three mobile phones.

There is a strict no mobile phone policy for students. Any student who wishes to bring a phone with them to May Blossom Farm must hand their phone in to the staff office on arrival where it will be locked away and returned to them when leaving the premises.

## 2. Scope

This policy applies to:

- All **students** attending Alternative Provision at May Blossom Farm
- All **staff**, including teaching, support, admin, volunteers, and contractors.
- Any **third parties** using or accessing ICT systems within our organisation.

It covers use of:

- The Secure File Server on the MBF Network
- Internet and email systems
- Service provided devices e.g. laptops, tablets, mobile phones
- Cloud-based systems e.g. Office 365, Google Workspace
- Mobile devices and communication platforms
- Filtering, supervision, monitoring, and data protection mechanisms

## 3. Principles

- ICT systems must be used in a way that upholds safeguarding, data protection, and professional standards at all times.

- Use of ICT is a privilege, not a right. Misuse may result in disciplinary or legal action.
- **Filtering, real time supervision and monitoring** systems are in place (see filtering, supervision and monitoring sub-section) to protect students from harmful or inappropriate content.
- **Staff must not use personal devices** for any work-related activities under any circumstances. If staff are found to be using their personal devices this may result in disciplinary action.

## 4. ICT Usage for Students

### 4.1 Acceptable Use

Students are expected to:

- Use May Blossom Farm ICT systems for educational purposes only.
- Access only appropriate and authorised websites, applications, and platforms.
- Report any accidental access to inappropriate content to the DSL as soon as possible.
- Treat May Blossom Farm devices and equipment with care.
- Use only their own individual logins and keep passwords secure at all times.

### 4.2 Prohibited Use

Students must not:

- Access or attempt to access websites containing extremist, pornographic, violent, or otherwise harmful content.
- Bypass or attempt to bypass filtering or security settings.
- Use devices to bully, harass, or threaten others (including via social media or messaging apps).
- Use another person's login credentials.
- Download or install unauthorised software or applications.

## 5. ICT Usage for Staff

### 5.1 Acceptable Use

Staff are expected to:

- Use May Blossom Farm devices and platforms for educational and professional purposes only.
- Communicate with students, parents, and colleagues only through authorised channels (e.g.email, approved platforms).
- Use password-protected accounts and lock screens when not in use.
- Ensure any sensitive or confidential data is stored in line with the Data Protection Policy and not on external devices or personal storage.

### 5.2 Prohibited Use

Staff must not:

- Download or store any May Blossom Farm related work including communication, planning, storing data on their **personal devices** (phones, tablets, laptops) accessing May Blossom Farm systems. NB during our start-up phase, until such time as we can afford dedicated laptops for both the DSL and DDSL, we will apply the Interim Personal Device Use addendum set out at Appendix 2.
- Share work related content or student information via personal email, messaging apps, or social media.
- Bypass May Blossom Farm filtering or security controls.
- Store student information on USB drives or other removable media not encrypted and approved by the IT Manager.

## 6. Filtering, Supervision and Monitoring (In Line with KCSIE)

In line with **KCSIE** requirements, May Blossom Farm has:

- Proportionate systems for the size and risk level of May Blossom Farm Provision
- An **approved web filtering system called DNS** that blocks access to illegal, inappropriate, or harmful online content including adult material, extremism, gambling and proxy sites. Filtering applies at Virtual Local Access Network level to all devices used by students.
- Strict staff supervision in place when students are working from iPads. Screens will be positioned so staff can see all online activity, visually observing the screens. Regular verbal checks, for example, 'Tell me what you're working on?' Review of browser history when any concern arises.
- Staff monitoring of student usage (e.g. checking search history and caches) which may be necessary if there is a concern.
- Acceptable use agreements and review of activity where concerns are identified.
- Apple devices (2 iPads) have been configured to block adult websites, restrict app downloads and disable private browsing. Students only have access to 2 iPads and cannot sign in with personal accounts that bypass controls.
- Regular termly reviews conducted by the IT Manager in consultation with the DSL ensure filtering settings remain appropriate and responsive to emerging threats. Admin access to filtering is the responsibility of the IT Manager. A record will be kept of these reviews.
- An incident response protocol for any breach or concern identified by staff. The DSL will also conduct random spot checks or checks when staff report a change in behaviour that warrants further investigation. This will include browser history and caches.

In line with **KCSIE** requirements, May Blossom Farm is working towards supplementing the above, when finances allow, with:

- An upgraded **filtering system** e.g. Lightspeed that tracks online activity on May Blossom Farm devices to detect potential safeguarding concerns/concerning behaviour, such as bullying, grooming, radicalisation, or exposure to harmful content.
- **This will log online activity, enabling it to be reviewed where appropriate by the Designated Safeguarding Lead (DSL).**

## 7. Cybersecurity and Data Protection

- Staff must follow the **Data Protection and GDPR Policy** at all times [Sept 2025 MBF Data Protection Policy.docx](#)
- Only secure, password protected systems should be used to store or share personal or confidential information.
- Staff must not email sensitive student information unless it is password protected.
- Lost or stolen devices or forgotten passwords must be reported immediately to the DSL and IT Manager.
- All passwords should be changed every 3 months to prevent Wifi use falling into unauthorised hands.
- Staff and students will receive regular training on data protection, phishing, and cyber risks. For further information on staff training see [Sept 2025 MBF Staff Induction Policy.docx](#)

## 8. Breaches and Consequences

### For Students:

- Minor breaches will be dealt with through internal behaviour procedures.
- Serious or repeated misuse may result in restricted access, suspension, or permanent courses withdrawal depending on the severity.

### For Staff:

- Any breach may be investigated under the Staff Code of Conduct Policy.
- Use of personal devices for work will be treated as a serious data protection and safeguarding breach.

## 9. Training and Awareness

- All staff receive regular training on acceptable ICT use, filtering, supervision, monitoring, and safeguarding online [Sept 2025 MBF Staff Induction Policy.docx](#)
- Students receive digital literacy and online safety education as part of the SEMH curriculum.
- This policy is reviewed during induction and annually thereafter.

## 10. Review of Systems

- The IT Manager will review online safeguarding controls annually.
- The DSL will review online safeguarding systems at least annually.
- Filtering systems are reviewed and tested quarterly.

## 11. Review of this Policy

- This policy will be reviewed annually or sooner if required by legislative or organisational changes.

**Related Policies**

- Safeguarding and Child Protection Policy
- Positive Relationships Policy
- Data Protection & GDPR Policy
- Staff Code of Conduct
- Acceptable Use and Mobile Phone Policy
- Staff Induction Policy

## **APPENDIX 1**

### **Incident Response Protocol**

This protocol outlines the steps taken by the provision when an online safety concern or incident is identified, in line with our safeguarding duties and the use of DNS-based filtering.

This approach applies to all staff, learners, and devices accessing the provision's internet network. It is considered **proportionate to the size, nature, and risk profile of the provision**, in line with statutory safeguarding guidance.

This protocol applies when:

- A learner attempts to access blocked or inappropriate content
- A learner reports encountering distressing or harmful material
- Staff observe concerning online behaviour
- There is suspicion of:
  - ✗ Sexual content
  - ✗ Extremism or radicalisation
  - ✗ Violence
  - ✗ Gambling
  - ✗ Self-harm or suicide-related content
  - ✗ Attempts to bypass filtering (VPNs, proxies)
- A safeguarding concern arises that has an online element

### **Detection of incidents**

Incidents may be identified through:

- DNS block notifications or (when the DNS system is upgraded) logs
- Staff supervision (real-time supervision of screens) during internet use
- Monitoring of browser history or device activity after internet use
- Learner self-reporting
- Behavioural changes linked to online activity

### **Immediate response (on the day)**

When an incident is identified, staff will:

1. **Ensure the learner's immediate safety**
  - ✓ Stop access to the device if necessary

- ✓ Offer reassurance and support
- ✓ Do not allow further access until reviewed

## 2. Preserve evidence

- ✓ Do not delete browser history or logs
- ✓ Note:
  - Date and time
  - Device used
  - Nature of content (no screenshots of illegal content)
- ✓ If DNS logs are relevant, ensure they are retained

## 3. Report to the Designated Safeguarding Lead (DSL) immediately

- ✓ Verbally where possible
- ✓ Followed by a written record

### **Role of the Designated Safeguarding Lead (DSL)**

The DSL will:

- ✓ Review the incident details and context
- ✓ Assess:
  - Level of risk
  - Intent vs accidental access
  - Any wider safeguarding concerns
- ✓ Decide on next steps in line with safeguarding procedures

### **Investigation and assessment**

The DSL may:

- ✓ Review DNS filtering categories and logs
- ✓ Check device/browser history
- ✓ Speak with:
  - The learner (age-appropriate, supportive)
  - Relevant staff members
- ✓ Consider whether:
  - Filtering settings need adjustment
  - The incident indicates emerging safeguarding risks

## **Response Actions**

Depending on the nature and severity of the incident, actions may include:

### **Low-level / accidental access**

- Reinforce acceptable use expectations
- Provide age-appropriate online safety guidance
- Record incident and outcome

### **Repeated or concerning access**

- Temporary restriction of internet access
- Increased supervision
- Parent/carer discussion (where appropriate)
- Safeguarding monitoring plan (to check browsing history and device activity)

### **Serious safeguarding concern**

- Follow safeguarding policy procedures
- Referral to:
  - Local Authority safeguarding team
  - Prevent (if extremism-related)
  - Children's Social Care
- Escalation to trustees/directors if required

### **Technical response (DNS-specific)**

Following an incident, the DSL or nominated IT lead will:

- Review DNS settings to ensure:
  - Relevant categories are blocked
  - Proxy/VPN sites remain blocked
  - SafeSearch enforcement is active
- Add specific domains to the **custom block list** if needed
- Document any changes made

### **Recording and documentation**

All incidents will be recorded using the provision's safeguarding recording system and will include:

- Description of the incident
- How it was identified

- Actions taken
- Outcome and follow-up
- Any technical changes made
- Name of staff and DSL involved

Records are stored securely and reviewed as part of safeguarding oversight.

### **Review and learning**

- Incidents are reviewed termly by the DSL
- Patterns or repeated issues inform:
- Staff training needs
- Updates to filtering settings
- Policy review

This protocol is reviewed **annually** or following a serious incident

### **Roles and responsibilities**

#### **All staff:**

- Supervise internet use
- Report concerns immediately
- Follow this protocol

#### **DSL:**

- Lead response and decision-making
- Liaise with external agencies
- Oversee filtering supervision and monitoring arrangements

#### **IT Manager:**

- Maintain DNS configuration
- Support evidence gathering

## **APPENDIX 2**

### **Interim Personal Device Use Addendum**

#### **Purpose of This Addendum**

May Blossom Farm CIC recognises that, due to the infancy of the Alternative Provision and current financial constraints, organisational work devices (e.g. laptops) are not yet available for all staff.

This addendum sets out strict safeguarding, data protection, and online safety controls governing the temporary and limited use of personal devices for work purposes.

This arrangement is exceptional, time-limited, and risk-managed, and does not replace the organisation's commitment to providing secure work devices as soon as is reasonably practicable.

#### **Scope**

This addendum applies only to:

- The DSL and DDSL
- Staff explicitly authorised by the Board of May Blossom Farm CIC

Personal devices include:

- Laptops

No other staff may use personal devices for work without written authorisation.

#### **Core Safeguarding Principle**

The welfare, privacy, and safety of children and young people remain paramount.

Personal devices (laptops) may only be used where:

- There is no reasonable alternative, and
- Safeguarding and data protection risks are actively mitigated.

#### **Permitted Use (Strictly Limited)**

Authorised staff may use personal devices (laptop) only for:

- Accessing work email via secure web-based platforms
- Accessing May Blossom Farm cloud systems (e.g. Google Workspace / Microsoft 365)
- Drafting planning documents within approved cloud platforms

All access must be:

- Browser-based
- Password protected
- Logged and auditable where possible

#### **Prohibited Use (Non-Negotiable)**

The following remain strictly prohibited, in line with the Online Safety Policy:

- Downloading, saving, or storing any May Blossom Farm work, communications, or student data on personal devices
- Storing student information locally, including:
  - Documents
  - Screenshots
  - Photos
  - Cached files
- Using personal email accounts, messaging apps (e.g. WhatsApp), SMS, or social media for work-related communication
- Recording meetings or interactions with students
- Using USB drives or removable media to store student information
- Bypassing organisational filtering, security, or access controls

Any breach must be reported immediately to the DSL.

### **Device Safeguarding Requirements**

Any personal device used must meet all of the following standards:

- Password, PIN, or biometric protection enabled
- Automatic screen lock set to a maximum of 5 minutes
- Up-to-date operating system and antivirus protection
- Device is not shared with family members or others
- Device is used in a private, secure environment (not public spaces)
- Screens must not be visible to others

Devices that do not meet these standards must not be used.

### **Safeguarding Boundaries (Alternative Provision Context)**

- No online contact with students may take place from bedrooms or private personal spaces
- Neutral backgrounds must be used where online communication occurs
- No images or video of students may be captured or stored on personal devices
- All communication with students must be logged centrally

### **Data Protection and Accountability**

- A Data Protection Impact Assessment (DPIA) has been completed to reflect this interim arrangement
- All authorised staff must sign a Personal Device Use Declaration confirming compliance
- Any loss, theft, or suspected data breach must be reported immediately to the DSL

### **Review and Time Limitation**

This addendum is temporary and will be reviewed by Russel Breyer,

**Review date: September 1<sup>st</sup> 2026**

The organisation is actively working towards the provision of dedicated work devices.

This arrangement will be withdrawn once organisational devices are available or if safeguarding risks cannot be adequately managed.

## 10. Approval

Approved by: Russel Breyer

Role: Designated Safeguarding Trustee

Date: 30.01.2026

## Data Protection Impact Assessment (DPIA)

Interim Use of Personal Devices (Laptops Only)

May Blossom Farm CIC – Alternative Provision

**Date completed:**

**Review date:** 1 September 2026

**Completed by:** Mr Russel Breyer (Designated Safeguarding Trustee)

## 1. Processing Overview

May Blossom Farm CIC's Online Safety Policy (Section 5.2) prohibits the use of personal devices for work purposes. However, due to the infancy of the provision and current financial constraints, organisational work laptops are not yet available.

As an **exceptional and interim measure**, the DSL, DDSL and Board-authorized staff are required to use personal laptops to access essential safeguarding and operational systems, in line with **Appendix 2: Interim Personal Device Use Addendum**.

No student data is intentionally downloaded, stored, or retained on personal devices.

## 2. Purpose and Necessity

This processing is necessary to:

- Maintain statutory safeguarding oversight
- Enable secure access to cloud-based systems
- Support operational continuity and leadership accountability

Without this interim arrangement, May Blossom Farm CIC would be unable to discharge its safeguarding and governance responsibilities effectively.

### 3. Lawful Basis

Processing is carried out under:

- **UK GDPR Article 6(1)(c)** – Legal obligation (safeguarding duties)
- **UK GDPR Article 6(1)(e)** – Public task
- **UK GDPR Article 9(2)(g)** – Substantial public interest (safeguarding children)

### 4. Data Involved

Data accessed may include:

- Student names and identifiers
- Safeguarding records and concerns
- Attendance and engagement information

Special category data may be accessed **via secure systems only** and is **not stored locally** on personal devices.

### 5. Identified Risks

<b>Risk</b>	<b>Potential Impact</b>
Loss or theft of device	Unauthorised data access
Accidental local storage	Data breach
Shared device use	Confidentiality breach
Insecure environments	Visual data exposure

### 6. Risk Mitigation Measures

Controls in place include:

- Personal devices restricted to **laptops only**
- Use limited to DSL, DDSL and Board-authorised staff
- Browser-based access to approved cloud platforms only
- No downloading, saving, screenshots, or offline access
- No use of personal email, messaging apps, or social media
- Password protection, automatic screen locking ( $\leq 5$  minutes), and antivirus required
- Devices not shared and not used in public spaces
- No recording or storage of student images or video

- All staff sign a Personal Device Use Declaration
- Immediate reporting of any loss, theft, or breach

### 7. Safeguarding Considerations (Alternative Provision)

- No online contact with students from bedrooms or private spaces
- Neutral backgrounds required
- All communication logged centrally
- Safeguarding oversight retained by the DSL

These measures ensure risk is **proportionate and controlled**.

### 8. Residual Risk Assessment

Residual risk level after mitigation:

Low     Medium     High

Risk is accepted **temporarily**, reviewed regularly, and linked to a clear exit strategy.

### 9. Review and Exit Strategy

This DPIA will be reviewed by the Designated Safeguarding Trustee and DSL by **1 September 2026**, or sooner if:

- Safeguarding risk increases
- A data breach occurs
- Organisational devices become available

The DPIA will be withdrawn once personal device use ceases.

#### Signed:

Russel Breyer



**Role:** Designated Safeguarding Trustee

**Date:** 30 January 2026

## Personal Device Use Declaration

### Interim Measure – May Blossom Farm CIC

**Name:** Gill Press

**Role:** Alternative Provision Lead and DSL

**Authorised by Mr Russel Breyer (Designated Safeguarding Trustee):**

**Date:** 30 January 2026

### Declaration

I acknowledge that May Blossom Farm CIC's **Online Safety Policy (Section 5.2)** prohibits the use of personal devices for work purposes.

I understand that, due to the infancy of the Alternative Provision and current financial constraints, I have been **explicitly authorised** to use my personal **laptop only** as a **temporary and exceptional measure**, in line with:

- Appendix 2: *Interim Personal Device Use Addendum*
- Data Protection Impact Assessment (DPIA)
- Safeguarding and Child Protection Policy

### Conditions of Use (Mandatory)

By signing this declaration, I confirm that:

#### 1. Device Security

- My device is password, PIN, or biometric protected
- Automatic screen lock is enabled (maximum 5 minutes)
- Operating system and antivirus software are up to date
- My device is **not shared** with family members or others

#### 2. Data Handling

I will **not**:

- Download, save, store, screenshot, or cache any May Blossom Farm work or student information
- Store student data locally in any format
- Use USB drives or removable media
- Enable offline access or syncing

All access will be:

- Browser-based
- Via approved cloud systems only

### 3. Communication

I will **only** use authorised platforms for work communication and will **not** use:

- Personal email accounts
- Messaging apps (e.g. WhatsApp, SMS)
- Social media

### 4. Safeguarding Boundaries

- I will not communicate with students from bedrooms or private personal spaces
- I will use neutral backgrounds for any online communication
- I will not record meetings or interactions
- I will not capture or store images or video of students
- All student communication will be logged centrally

### 5. Environment

- My device will only be used in secure, private environments
- Screens will not be visible to unauthorised individuals
- I will not use public Wi-Fi or public spaces for work access

### 6. Reporting and Accountability

- I will report **immediately** to the DSL any:
  - Loss or theft of my device
  - Suspected data breach
  - Accidental access, storage, or disclosure of information

I understand that:

- Any breach may be treated as a **safeguarding and data protection incident**
- Failure to comply may result in disciplinary action

### Confirmation

I confirm that I have read, understood, and agree to comply with all conditions outlined above.

I understand this authorisation is **temporary**, subject to review, and will be withdrawn once organisational devices are available or if safeguarding risks cannot be adequately managed.

A handwritten signature in black ink, consisting of several loops and a final horizontal stroke.

**Signed:**

**Date:** 30 January 2026

## Personal Device Use Declaration

### Interim Measure – May Blossom Farm CIC

**Name:** John Frenett

**Role:** Alternative Provision joint-proprietor and DDSL

**Authorised by Mr Russel Breyer (Designated Safeguarding Trustee):**

**Date:** 30 January 2026

### Declaration

I acknowledge that May Blossom Farm CIC's **Online Safety Policy (Section 5.2)** prohibits the use of personal devices for work purposes.

I understand that, due to the infancy of the Alternative Provision and current financial constraints, I have been **explicitly authorised** to use my personal **laptop only** as a **temporary and exceptional measure**, in line with:

- Appendix 2: *Interim Personal Device Use Addendum*
- Data Protection Impact Assessment (DPIA)
- Safeguarding and Child Protection Policy

### Conditions of Use (Mandatory)

By signing this declaration, I confirm that:

#### 1. Device Security

- My device is password, PIN, or biometric protected
- Automatic screen lock is enabled (maximum 5 minutes)
- Operating system and antivirus software are up to date
- My device is **not shared** with family members or others

#### 2. Data Handling

I will **not**:

- Download, save, store, screenshot, or cache any May Blossom Farm work or student information
- Store student data locally in any format
- Use USB drives or removable media
- Enable offline access or syncing

All access will be:

- Browser-based
- Via approved cloud systems only

### 3. Communication

I will **only** use authorised platforms for work communication and will **not** use:

- Personal email accounts
- Messaging apps (e.g. WhatsApp, SMS)
- Social media

### 4. Safeguarding Boundaries

- I will not communicate with students from bedrooms or private personal spaces
- I will use neutral backgrounds for any online communication
- I will not record meetings or interactions
- I will not capture or store images or video of students
- All student communication will be logged centrally

### 5. Environment

- My device will only be used in secure, private environments
- Screens will not be visible to unauthorised individuals
- I will not use public Wi-Fi or public spaces for work access

### 6. Reporting and Accountability

- I will report **immediately** to the DSL any:
  - Loss or theft of my device
  - Suspected data breach
  - Accidental access, storage, or disclosure of information

I understand that:

- Any breach may be treated as a **safeguarding and data protection incident**
- Failure to comply may result in disciplinary action

### Confirmation

I confirm that I have read, understood, and agree to comply with all conditions outlined above.

I understand this authorisation is **temporary**, subject to review, and will be withdrawn once organisational devices are available or if safeguarding risks cannot be adequately managed.



**Signed:**

**Date:** 30 January 2026

## Personal Device Use Declaration

### Interim Measure – May Blossom Farm CIC

**Name:** Hannah Priest

**Role:** Alternative Provision deputy lead, joint-proprietor and DDSL

**Authorised by Mr Russel Breyer (Designated Safeguarding Trustee):**

**Date:** 30 January 2026

### Declaration

I acknowledge that May Blossom Farm CIC's **Online Safety Policy (Section 5.2)** prohibits the use of personal devices for work purposes.

I understand that, due to the infancy of the Alternative Provision and current financial constraints, I have been **explicitly authorised** to use my personal **laptop only** as a **temporary and exceptional measure**, in line with:

- Appendix 2: *Interim Personal Device Use Addendum*
- Data Protection Impact Assessment (DPIA)
- Safeguarding and Child Protection Policy

### Conditions of Use (Mandatory)

By signing this declaration, I confirm that:

#### 1. Device Security

- My device is password, PIN, or biometric protected
- Automatic screen lock is enabled (maximum 5 minutes)
- Operating system and antivirus software are up to date
- My device is **not shared** with family members or others

#### 2. Data Handling

I will **not**:

- Download, save, store, screenshot, or cache any May Blossom Farm work or student information
- Store student data locally in any format
- Use USB drives or removable media
- Enable offline access or syncing

All access will be:

- Browser-based
- Via approved cloud systems only

### 3. Communication

I will **only** use authorised platforms for work communication and will **not** use:

- Personal email accounts
- Messaging apps (e.g. WhatsApp, SMS)
- Social media

### 4. Safeguarding Boundaries

- I will not communicate with students from bedrooms or private personal spaces
- I will use neutral backgrounds for any online communication
- I will not record meetings or interactions
- I will not capture or store images or video of students
- All student communication will be logged centrally

### 5. Environment

- My device will only be used in secure, private environments
- Screens will not be visible to unauthorised individuals
- I will not use public Wi-Fi or public spaces for work access

### 6. Reporting and Accountability

- I will report **immediately** to the DSL any:
  - Loss or theft of my device
  - Suspected data breach
  - Accidental access, storage, or disclosure of information

I understand that:

- Any breach may be treated as a **safeguarding and data protection incident**
- Failure to comply may result in disciplinary action

### Confirmation

I confirm that I have read, understood, and agree to comply with all conditions outlined above.

I understand this authorisation is **temporary**, subject to review, and will be withdrawn once organisational devices are available or if safeguarding risks cannot be adequately managed.

**Signed:** *Hannah Priest*

**Date:** 30 January 2026