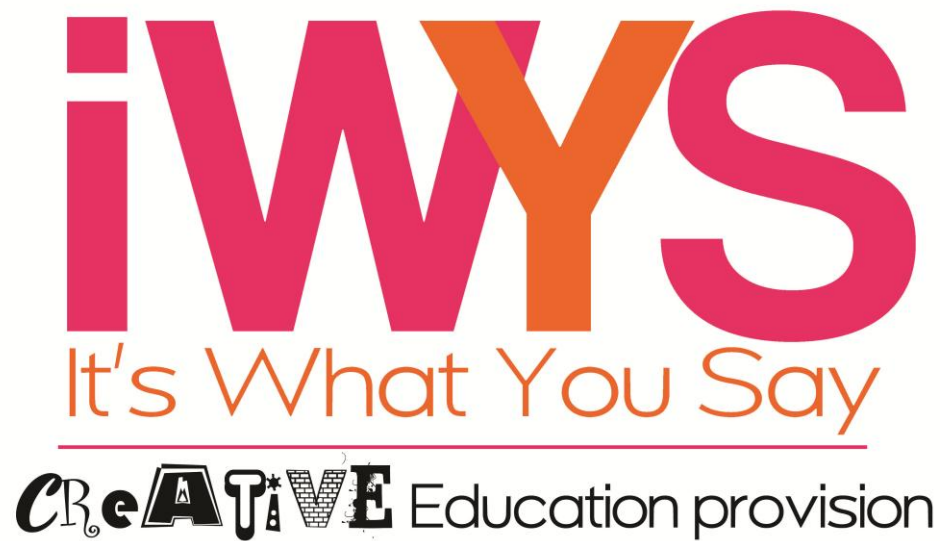




IWYS ALTERNATIVE PROVISION INFORMATION SECURITY POLICY

Document Control

Policy title	Information Security Policy
Organisation	IWYS Alternative Provision
Policy period	2026 / 2027
Approved by	Charmaine Baines – Head of Provision / Proprietor
Date approved	October 2026
Review date	October 2027

Related legislation and guidance: UK GDPR and Data Protection Act 2018; Computer Misuse Act 1990; Freedom of Information Act 2000 where applicable; safeguarding requirements; Department for Education guidance on cyber security and data protection; and Keeping Children Safe in Education (KCSIE), as applicable to the current policy year.

Contents

1. Policy Statement
2. Purpose and Objectives
3. Scope
4. Information Security Principles
5. Roles and Responsibilities
6. Information Classification and Handling
7. Access Control and User Accounts
8. Passwords and Multi-Factor Authentication
9. Devices, Equipment and Removable Media
10. Email, Internet and Cloud Services
11. Remote Working and Home Working
12. Data Protection and Confidential Information
13. Safeguarding and Information Security
14. Cyber Security and Malware Protection
15. Backups, Business Continuity and Recovery
16. Security Incidents and Data Breaches
17. Physical Security
18. Third-Party Suppliers and Contractors
19. Staff Training and Awareness
20. Monitoring and Acceptable Use
21. Non-Compliance
22. Policy Review

Appendix A – Information Security Incident Reporting

Appendix B – Staff Information Security Checklist

Appendix C – Key Contacts and Escalation

1. Policy Statement

IWYS Alternative Provision recognises that information is a valuable organisational asset and that the confidentiality, integrity and availability of information are essential to the safe and effective operation of the provision.

IWYS is committed to protecting personal, safeguarding, educational, financial, operational and commercially sensitive information from unauthorised access, accidental loss, inappropriate disclosure, alteration, destruction, malware, cyber attack and other security threats.

Information security is the responsibility of everyone who uses IWYS information, systems or equipment. The organisation will apply proportionate technical, physical and organisational controls and will promote a culture in which security concerns are reported promptly.

2. Purpose and Objectives

The purpose of this policy is to establish clear requirements for protecting IWYS information and information systems.

Objectives include:

- protect children, young people, staff, visitors and other individuals whose information is held by IWYS;
- prevent unauthorised access, disclosure, alteration or destruction of information;
- support compliance with data protection, safeguarding and other applicable legal requirements;
- reduce the likelihood and impact of cyber security incidents;
- ensure information is available to authorised users when required for education, safeguarding and business continuity;
- provide a clear process for reporting, responding to and learning from security incidents.

3. Scope

This policy applies to all staff, tutors, volunteers, agency workers, contractors, visitors and other authorised users who access IWYS information or systems. It applies to information in paper and electronic form and to IWYS-owned or authorised personal devices used for work.

- student and parent/carer information;
- safeguarding and child protection records;
- staff and recruitment information;
- attendance, assessment and education records;
- financial and contractual information;
- emails, documents, photographs, recordings and other digital content;
- cloud platforms, databases, websites, networks, laptops, tablets, phones and removable media.

4. Information Security Principles

IWYS will apply the following principles:

- Confidentiality – information is only accessible to people who are authorised to receive it.
- Integrity – information is accurate, complete and protected from unauthorised alteration.
- Availability – authorised users can access information and systems when needed.
- Data minimisation – only information necessary for a legitimate purpose should be collected, accessed or retained.
- Need-to-know access – access rights will reflect job responsibilities and safeguarding requirements.
- Secure by default – security considerations will be included when introducing systems, devices, suppliers or processes.

5. Roles and Responsibilities

5.1 Senior Leadership

- provide leadership and resources for information security;
- ensure significant security risks are identified and managed;
- ensure serious incidents are escalated appropriately;
- ensure this policy is reviewed and implemented.

5.2 Information Security / Data Protection Lead

- maintain the information security framework and associated procedures;
- support incident management and data breach assessment;
- coordinate training and awareness;
- review access arrangements and security controls;
- liaise with relevant external advisers, suppliers or authorities where required.

5.3 All Staff and Users

- keep passwords and authentication information secure;
- use only authorised systems and software;
- protect confidential information from unauthorised disclosure;
- lock screens and secure devices when unattended;
- report suspected phishing, malware, lost devices, accidental disclosure or other security incidents immediately;
- complete required information security and safeguarding training.

6. Information Classification and Handling

Information should be handled according to its sensitivity. As a minimum, staff should distinguish between:

Classification	Examples	Handling
Public	Approved website or promotional information.	May be shared publicly once authorised.
Internal	Routine operational information.	Share only with appropriate staff or authorised recipients.
Confidential	Student, staff, financial or contractual information.	Need-to-know access; use secure systems and approved transmission methods.
Highly Confidential / Special Category	Safeguarding, health, biometric or other particularly sensitive information.	Strict access control; secure storage/transmission; disclose only where lawful and necessary.

7. Access Control and User Accounts

- Users must have individual accounts wherever the system permits; shared accounts should be avoided unless there is a documented operational reason.
- Access should be granted according to role and legitimate need.
- Accounts must be removed or disabled promptly when a user leaves or no longer requires access.
- Access rights should be reviewed periodically and following significant role changes.
- Users must not attempt to bypass security controls or access information outside their authorised role.
- Administrator privileges should be restricted to authorised personnel and used only when required.

8. Passwords and Multi-Factor Authentication

- Use strong, unique passwords for IWYS accounts.
- Never share passwords or authentication codes with another person.
- Do not reuse an IWYS password for unrelated personal services.
- Where available and appropriate, multi-factor authentication (MFA) should be enabled, particularly for administrative, cloud and remote-access accounts.
- Passwords suspected of compromise must be changed immediately and the incident reported.
- Password managers may be used where approved by IWYS.

9. Devices, Equipment and Removable Media

- Only authorised and appropriately protected devices should be used to access IWYS systems.
- Devices should use supported operating systems, security updates and anti-malware protections.
- Screens must be locked when devices are unattended.
- Laptops and mobile devices containing confidential information must be physically secured when not in use.
- Lost or stolen devices must be reported immediately.
- USB/removable media should be avoided for sensitive information unless authorised, encrypted where appropriate and required for a legitimate business purpose.

- Personal devices must not be used to store or transfer sensitive IWYS information unless specifically authorised and appropriately secured.

10. Email, Internet and Cloud Services

- Use IWYS-approved email and cloud services for organisational information.
- Check recipients carefully before sending confidential information.
- Use secure/encrypted methods where required for sensitive information.
- Treat unexpected links, attachments, requests for passwords, payment changes or urgent requests with caution.
- Do not install unauthorised software, browser extensions or applications on IWYS equipment.
- Do not use personal email or unapproved cloud storage for IWYS confidential information.
- Internet use must be lawful, appropriate and consistent with safeguarding and acceptable-use requirements.

11. Remote Working and Home Working

- Remote access must use authorised systems and secure connections.
- Confidential information must not be visible to unauthorised household members or members of the public.
- Paper records should not be removed from IWYS premises unless there is a legitimate need and appropriate controls are in place.
- Work devices must not be left unattended in vehicles or other insecure locations.
- Public or unsecured Wi-Fi should be used cautiously and preferably avoided for sensitive activity unless an approved secure connection is in place.

12. Data Protection and Confidential Information

IWYS will process personal information lawfully, fairly and transparently and will apply the principles of the UK GDPR and Data Protection Act 2018. Staff must follow the organisation's data protection and records management procedures.

- Only collect and access information necessary for the legitimate purpose.
- Keep information accurate and report inaccuracies promptly.
- Do not disclose personal information unless there is a lawful basis and the recipient is authorised.
- Use BCC or other appropriate controls where group email recipients should not see each other's addresses.
- Check attachments and recipients before sending sensitive information.
- Dispose of confidential paper securely and delete electronic information in accordance with retention requirements.

13. Safeguarding and Information Security

Information security forms part of IWYS safeguarding arrangements. Safeguarding information must be treated as highly confidential and shared only with appropriate people for legitimate safeguarding purposes.

- Concerns about unauthorised access to safeguarding records must be reported immediately to the Designated Safeguarding Lead (DSL) and appropriate information security/data protection lead.
- Staff must not discuss safeguarding cases in public areas or through unapproved messaging platforms.

- Images, recordings and student information must only be captured, stored and shared in accordance with IWYS procedures and consent/lawful-basis requirements.
- Online safety and cyber security concerns involving students must be considered within the wider safeguarding framework.

14. Cyber Security and Malware Protection

- Security updates and patches should be applied promptly to supported devices and systems.
- Anti-malware and endpoint protections should be maintained where appropriate.
- Staff should not disable security software or firewall protections without authorisation.
- Suspected phishing or malware must be reported immediately; users should not continue interacting with suspicious content.
- Backups should be protected against unauthorised access and, where feasible, ransomware or accidental deletion.

15. Backups, Business Continuity and Recovery

- Important organisational information should be backed up using approved systems.
- Backups should be tested periodically to confirm that information can be recovered.
- Critical systems and information should be prioritised in business continuity arrangements.
- Where a cyber incident affects availability, staff should follow the emergency/business continuity procedure rather than attempting unauthorised recovery.

16. Security Incidents and Data Breaches

A security incident includes any actual or suspected loss, theft, unauthorised access, accidental disclosure, phishing attack, malware infection, compromised account, lost device, inappropriate sharing or other event that could affect information security.

1. Report the incident immediately to the appropriate senior lead, information security/data protection lead and, where relevant, the DSL.
2. Take reasonable steps to contain the incident without destroying evidence.
3. Do not attempt to conceal the incident or delay reporting while investigating it yourself.
4. The organisation will assess the incident, including whether it constitutes a personal data breach and whether notification to the ICO, affected individuals, police, insurers, suppliers or other bodies is required.
5. The incident will be documented and reviewed to identify lessons and preventative actions.

Where a personal data breach is likely to result in a risk to individuals' rights and freedoms, IWYS will consider the applicable UK GDPR reporting requirements and timescales.

17. Physical Security

- Access to offices, classrooms, server/network equipment and records areas should be controlled.
- Visitors must follow IWYS visitor procedures and must not be given unsupervised access to confidential records or systems unless authorised.
- Paper records must be stored securely when not in use.
- Keys, access cards and alarm/security information must be protected and returned when no longer required.

- Equipment disposal must ensure information cannot be recovered.

18. Third-Party Suppliers and Contractors

- Suppliers handling IWYS information must be appropriately assessed and, where required, covered by contractual data protection and confidentiality provisions.
- Access should be limited to what the supplier needs to perform its role.
- Third-party accounts and access should be removed when no longer required.
- Security requirements should be considered when procuring software, cloud services, devices or other technology.

19. Staff Training and Awareness

IWYS will provide appropriate information security and data protection awareness to staff and other relevant users. Training should include phishing awareness, password security, safe handling of personal information, reporting incidents and safeguarding considerations.

- Induction training for new staff and relevant contractors.
- Refresher training at appropriate intervals.
- Additional training following significant incidents or identified risks.

20. Monitoring and Acceptable Use

- IWYS may monitor use of its systems, networks and devices where lawful, proportionate and necessary for security, safeguarding, operational or compliance purposes.
- Monitoring will be conducted in accordance with applicable privacy and data protection requirements.
- Users must not use IWYS systems to access, create, store or distribute unlawful, discriminatory, abusive or otherwise inappropriate material.
- Security logs and audit information may be retained for an appropriate period to support investigation and compliance.

21. Non-Compliance

Failure to comply with this policy may expose IWYS, students, staff and others to significant risk. Depending on the circumstances, non-compliance may result in additional training, removal of access, disciplinary action, contractual action, referral to safeguarding leads, or notification to relevant authorities.

Serious or deliberate misuse of systems, unauthorised access, deliberate disclosure of confidential information or attempts to circumvent security controls may constitute a disciplinary matter and/or an offence.

22. Policy Review

This policy will be reviewed at least annually and sooner where there are significant changes to legislation, DfE guidance, technology, organisational arrangements or the threat environment. Lessons from incidents, audits and risk assessments will be used to improve the policy and associated procedures.

Appendix A – Information Security Incident Reporting

Use this checklist when an information security incident is suspected.

Action	Completed / Notes
Date/time of incident identified	
Person reporting incident	
System/device/information affected	
Nature of incident (lost device / phishing / malware / disclosure / unauthorised access / other)	
Immediate containment action taken	
Senior lead / Information Security Lead informed	
DSL informed where safeguarding information is involved	
Data protection breach assessment completed	
External notification considered / made	
Incident recorded	
Lessons learned / corrective actions	

Appendix B – Staff Information Security Checklist

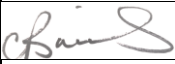
- I use a strong, unique password for IWYS systems.
- I do not share passwords or authentication codes.
- I lock my screen whenever I leave a device unattended.
- I check recipients and attachments before sending emails.
- I use only approved systems for confidential IWYS information.
- I know how and where to report a suspected cyber security incident.
- I know that safeguarding information must be shared only on a need-to-know basis.
- I keep IWYS devices secure when working away from the provision.
- I do not install unauthorised software or disable security controls.
- I complete required information security and data protection training.

Appendix C – Key Contacts and Escalation

Role	Name	Contact details
Head of Provision / Proprietor	Charmaine Baines	Email: charmaine@iwys.co.uk Tel: 07341 213174
Information Security / Data Protection Lead	Charmaine Baines	Email: charmaine@iwys.co.uk Tel: 07341 213174
Designated Safeguarding Lead (DSL)	Charmaine Baines	Email: charmaine@iwys.co.uk Tel: 07341 213174
IT Support / Managed Service Provider	ICTN Filtering Service	Email: LCanry@ictn.co.uk Telephone: +44 (0) 1782 406406
Emergency / Police (where appropriate)	Staffordshire Police	999

Approval and Sign-Off

This policy has been reviewed and approved for use by IWYS Alternative Provision.

Approved by	Charmaine Baines
Role	Head of Provision/Proprietor
Signature	
Date	October 2026
Next review date	October 2027