



RESPECT. RESILIENCE. INTEGRITY.

Digital Technology, Young Person's Internet, Acceptable Use **and** Cyber Security Policy

DATE APPROVED

24 September 2026

NEXT DOCUMENT REVIEW

July 2027

Policy Owner:	Sam Gray, Headteacher
Confirmed by	Life Changing Education Ltd, acting through Krystian Liptrot, Chair of the proprietor board and company
Approval Status:	Approved
Date Approved:	24 September 2026
Date Implemented:	24 September 2026
Next document review	July 2027 (governors advise; proprietor decides)
Applies to:	Pupils, staff, volunteers, visitors, contractors and everyone using Academy digital systems or networks. Registered site: Unit 4, Howarth Court, Oldham Gateway, Gateway Crescent, Chadderton, Oldham, OL9 9XB.

LCE ACADEMY

Contents

1	Statement of Intent	4	15	Artificial Intelligence (AI)	12
2	Purpose	4	16	Microsoft 365, Google Workspace and Cloud Storage	14
3	Scope	5	17	CPOMS	14
4	Legal Framework	5	18	Digital Communication	14
5	Principles of Acceptable Use	6	19	Social Media	15
6	Roles and Responsibilities	6	20	Photography, Audio and Video Recording	15
7	Professional Conduct	8	21	Printing and Paper Records	16
8	User Accounts and Passwords	9	22	Removable Media	16
9	Academy Devices	9	23	Cyber Security	16
10	Personal Devices	9	24	Filtering and Monitoring	17
11	Mobile Phones	10	25	BluRock IT	17
12	Training	10	26	Business Continuity	18
13	Academy Email	11	27	Reporting Concerns	18
14	Internet Access	11			

28	Pupil Use of Technology	19	37	Training and Professional Development	22
29	Mobile Phones and Personal Devices	19	38	Monitoring and Quality Assurance	23
30	Digital Behaviour Expectations	19	39	Policy Review	23
31	Online Safety Education	20	A	Appendix A - Staff Digital Responsibility Checklist	25
32	Visitors and Contractors	20	B	Appendix B - Artificial Intelligence Checklist	25
33	Monitoring Use of Academy Systems	21	C	Appendix C - Young Person's Internet Policy and Digital Agreement	26
34	Misuse of Technology	21	D	Appendix D - Remote Working Checklist	26
35	Responding to Breaches	22	E	Appendix E - Policy Summary	27
36	Cyber Security Incidents	22			

1

Statement of Intent

Technology plays an essential role in delivering high-quality education, safeguarding children and supporting the efficient operation of LCE Academy.

The Academy recognises that digital technology creates significant opportunities to enhance teaching, learning, communication and administration. Equally, it presents risks relating to safeguarding, cyber security, confidentiality and professional conduct.

This policy establishes clear expectations for the safe, responsible and professional use of digital technology by all members of the Academy community.

LCE Academy is committed to ensuring that:

- Technology enhances teaching and learning.
- Digital systems support effective safeguarding.
- Personal information remains secure.
- Staff use technology professionally and responsibly.
- Pupils develop safe and responsible digital behaviours.
- Cyber security risks are minimised.
- Technology is used in ways that reflect the Academy's values of Respect, Resilience and Integrity.

Every member of the Academy community shares responsibility for maintaining a secure digital environment.

2

Purpose

The purpose of this policy is to:

- Promote safe and responsible use of technology.
- Protect pupils, staff and visitors from digital risks.
- Safeguard personal information.
- Support compliance with UK GDPR and the Data Protection Act 2018.
- Maintain secure Academy systems.
- Promote cyber security awareness.
- Clarify expectations regarding professional conduct online.
- Reduce the likelihood of cyber security incidents.
- Support effective filtering and monitoring arrangements.

Scope

This policy applies to:

- Employees.
- Agency staff.
- Volunteers.
- Governors.
- Proprietor.
- Contractors.
- Students and students on placement.
- Visitors using Academy technology.
- External professionals accessing Academy systems.

The policy applies whenever Academy information is accessed using:

- Academy computers.
- Laptops.
- Tablets.
- Mobile phones.
- Personal devices authorised for Academy business.
- Cloud-based systems.
- Remote working arrangements.

The policy applies both on and off Academy premises whenever Academy systems or information are being accessed.

Legal Framework

This policy has been developed with reference to:

- Keeping Children Safe in Education 2026.
- UK GDPR.
- Data Protection Act 2018.
- Computer Misuse Act 1990.
- Copyright, Designs and Patents Act 1988.
- Communications Act 2003.
- Independent School Standards.
- DfE Filtering and Monitoring Standards.

- Cyber Essentials guidance.
- Information Commissioner's Office guidance.
- National Cyber Security Centre guidance.

Counter-Terrorism and Security Act 2015 and the Prevent Duty.

This policy should be read alongside the Academy's:

- Safeguarding and Child Protection Policy.
- Behaviour Policy.
- Staff Code of Conduct.
- Data Protection, Privacy and Information Governance Policy.
- Mobile-phone arrangements in the Behaviour Policy.
- Appendix D - Remote Working Checklist.

5 Principles of Acceptable Use

The Academy expects technology to be used:

- Safely.
- Professionally.
- Responsibly.
- Respectfully.
- Securely.
- Lawfully.
- Ethically.

Technology should always support education, safeguarding and the effective operation of the Academy.

Staff should consider whether their digital activity would withstand professional scrutiny if reviewed by colleagues, leaders, parents or external agencies.

6 Roles and Responsibilities

Proprietor body

Will ensure:

- Appropriate digital infrastructure is available.
- Cyber security risks are monitored.
- Policies remain compliant.
- Sufficient resources are allocated.

- Filtering and monitoring arrangements remain effective.

Headteacher

The Headteacher has overall responsibility for digital safety within the Academy.

Responsibilities include:

- Implementing this policy.
- Promoting safe technology use.
- Supporting cyber security.
- Ensuring staff training.
- Responding to serious breaches.
- Working with BluRock IT and other specialist providers.

Senior Leadership Team

Will support implementation through:

- Monitoring compliance.
- Supporting staff.
- Promoting effective digital practice.
- Coordinating staff training where appropriate.

Designated Safeguarding Lead

The Designated Safeguarding Lead will:

- Respond to online safeguarding concerns.
- Review filtering and monitoring alerts where appropriate.
- Work with Smoothwall and BluRock IT where safeguarding concerns arise.
- Ensure online risks are managed effectively.
- Record safeguarding concerns on CPOMS.

BluRock IT

BluRock IT provides technical support for the Academy.

Responsibilities include:

- Maintaining network security.
- Supporting cyber security measures.
- Applying software updates.
- Supporting secure user access.
- Monitoring system performance.
- Responding to technical incidents.

- Advising on digital resilience.

BluRock IT personnel may access Academy systems only where necessary to provide authorised technical support and are subject to appropriate confidentiality arrangements.

All Staff

All staff must:

- Follow this policy.
- Protect Academy information.
- Use technology professionally.
- Report concerns promptly.
- Complete mandatory training.
- Maintain secure passwords.
- Change passwords immediately where compromise is suspected or when directed following a security incident.
- Lock devices when unattended.
- Report lost or stolen devices immediately.
- Challenge unsafe practice where appropriate.

Technology should never be used in a manner that could undermine safeguarding, confidentiality or professional standards.

7 Professional Conduct

Staff should remember that professional standards apply equally online and offline.

Digital communication should always demonstrate:

- Professionalism.
- Respect.
- Confidentiality.
- Appropriate boundaries.

Staff must not:

- Communicate with pupils using personal social media accounts.
- Share confidential Academy information through unauthorised platforms.
- Post content that could damage the Academy's reputation.
- Use Academy technology for unlawful purposes.
- Access inappropriate material.
- Circumvent security controls.

Where uncertainty exists, staff should seek advice before proceeding.

8 User Accounts and Passwords

Each user will receive an individual account where appropriate.

Users must:

- Keep passwords confidential.
- Create strong passwords.
- Avoid sharing accounts.
- Change passwords if compromise is suspected.
- Enable multi-factor authentication where available.

Passwords must never be written where they can be easily accessed by others.

Shared accounts should only be used where specifically authorised.

9 Academy Devices

Academy devices remain the property of LCE Academy.

Users are expected to:

- Take reasonable care of equipment.
- Keep devices physically secure.
- Store devices safely.
- Install updates when prompted.
- Avoid unauthorised software installation.
- Return devices upon request or termination of employment.

Devices should not be left unattended in public places or visible inside vehicles.

10 Personal Devices

The Academy recognises that authorised staff may occasionally use personal devices for Academy business where this supports operational effectiveness.

Use of personal devices is permitted only where:

- It has been authorised by the Academy.
- Appropriate security measures are in place.
- The device is password protected.

- Academy information is stored only where approved.
- Personal data is protected in accordance with the Academy's Data Protection Policy.

Staff must not:

- Store safeguarding records permanently on personal devices.
- Store EHCP documentation locally.
- Photograph confidential documents for convenience.
- Use personal messaging applications to communicate with pupils.

Where Academy information is temporarily accessed on personal devices, it should be transferred to approved Academy systems as soon as reasonably practicable and removed from the personal device.

11 Mobile Phones

Pupils are required to hand in mobile phones at the beginning of each Academy day in accordance with the Academy's Behaviour Policy.

Staff may use mobile phones during the working day only where this is appropriate, professional and does not compromise supervision or safeguarding.

Personal use is limited to break times in non-pupil areas, except for authorised work, emergency or safeguarding use.

Photography or video recording of pupils must only take place using authorised Academy equipment unless specific authorisation has been given by the Headteacher.

12 Training

All staff will receive appropriate training covering:

- Cyber security.
- Password management.
- Phishing awareness.
- Safe technology use.
- Online safeguarding.
- Data protection.
- Acceptable use expectations.
- GDPR expectations and working practices

Training will form part of staff induction and will be refreshed regularly to reflect emerging risks and technological developments.

Academy Email

Academy email accounts are provided for professional communication and remain the property of LCE Academy.

Staff should use Academy email for all Academy business.

Users must:

- Check recipients carefully before sending emails.
- Ensure information shared is accurate and appropriate.
- Use professional language.
- Protect confidential information.
- Report suspicious emails immediately.
- Delete unnecessary emails in accordance with the Academy's retention arrangements.

Confidential or sensitive information should only be sent where there is a lawful purpose and appropriate security measures have been considered.

Staff must never use personal email accounts for routine Academy business.

Internet Access

Internet access is provided to support education, safeguarding and the effective operation of the Academy.

Users should access websites that are:

- Educational.
- Professional.
- Appropriate to their role.
- Safe and lawful.

Users must not:

- Access illegal material.
- Attempt to bypass filtering systems.
- Download unauthorised software.
- Visit inappropriate websites.
- Stream excessive personal entertainment.
- Use Academy systems for personal commercial activity.

Personal use is limited to break times in non-pupil areas, except for authorised work, emergency or safeguarding use, and must not interfere with professional responsibilities or compromise the security or reputation of the Academy.

Artificial Intelligence (AI)

LCE Academy recognises that Artificial Intelligence (AI) can improve efficiency, enhance teaching and support curriculum planning when used responsibly.

AI should complement professional judgement and should never replace it.

Approved AI tools may be used to support:

- Lesson planning.
- Resource creation.
- Curriculum design.
- Differentiation.
- Administrative tasks.
- Drafting reports and policies.
- Generating ideas and examples.
- Professional development.

All AI-generated content must be reviewed by the member of staff before use.

Staff remain professionally responsible for the accuracy, suitability and quality of any content produced with the assistance of AI.

Prohibited Use of AI

Staff must not upload or input into publicly available AI systems:

- Safeguarding records.
- CPOMS entries.
- EHCPs.
- Medical information.
- Behaviour records.
- Speech and Language Therapy reports.
- Educational Psychology reports.
- Personnel records.
- Personal data that could identify pupils, parents or staff.
- Confidential Academy information.

Information should only be entered into AI platforms where this complies with Academy guidance, UK GDPR and any contractual arrangements.

AI and Teaching

Teachers may use AI to enhance learning but should ensure that:

- Resources are age appropriate.
- Content is accurate.
- Bias is identified and removed where possible.
- Safeguarding considerations have been addressed.
- Materials remain aligned with the Academy curriculum.

AI should never replace high-quality teaching or professional expertise.

AI and Assessment

AI may support assessment by assisting staff with:

- Creating assessment materials.
- Developing success criteria.
- Producing model answers.
- Suggesting adaptive teaching strategies.

AI must not be used to make automated decisions regarding pupils' attainment, behaviour, safeguarding or educational provision.

Assessment decisions remain the responsibility of qualified professionals.

AI and Pupil Use

Pupils may use approved AI technologies where this forms part of planned learning.

Staff will teach pupils:

- How AI works.
- Its benefits and limitations.
- Responsible and ethical use.
- Critical evaluation of AI-generated content.
- Academic honesty.
- Safe online behaviour.

Any use of AI by pupils should be appropriately supervised.

Microsoft 365, Google Workspace and Cloud Storage

Google Workspace is the Academy's primary approved platform for school email, collaborative documents and controlled cloud storage. Microsoft 365 desktop applications may be used for approved school work; Microsoft cloud storage, Teams or other services are used only where they appear in the approved systems register with a defined purpose, access control, processor agreement, retention rule and staff guidance. Staff do not choose personal or unapproved cloud services for Academy information.

Users should:

- Store Academy documents within approved locations.
- Avoid creating unnecessary duplicates.
- Share documents securely.
- Apply appropriate permissions.
- Follow version control procedures where appropriate.

Personal cloud storage services must not be used to store confidential Academy information.

CPOMS

CPOMS is the Academy's designated safeguarding recording system.

Staff must alert the DSL or deputy without delay and record every pupil safeguarding concern factually on CPOMS as soon as reasonably practicable. Recording or submitting a CPOMS entry must never delay immediate protective or emergency action, and staff must check that urgent concerns have been received.

Staff must:

- Record information factually.
- Avoid opinion unless clearly identified.
- Complete records promptly.
- Maintain confidentiality.
- Never share CPOMS access credentials.

Information contained within CPOMS remains confidential and should only be accessed by authorised staff.

Digital Communication

Digital communication should reflect the same professional standards expected in face-to-face interactions.

This includes:

- Emails.
- Microsoft Teams.

- Video meetings.
- Online messaging systems.
- Digital learning platforms.

Staff should:

- Communicate respectfully.
- Maintain professional boundaries.
- Avoid unnecessary informal communication.
- Use Academy-approved platforms.

19 Social Media

Staff should remember that online activity may affect public confidence in the Academy.

Staff must not:

- Identify pupils without authorisation.
- Discuss Academy matters publicly.
- Share confidential information.
- Comment on safeguarding matters.
- Engage in online disputes relating to the Academy.
- Contact pupils using personal social media accounts.

Personal social media use remains a private matter but staff should recognise that inappropriate online behaviour may affect professional relationships and the reputation of the Academy.

20 Photography, Audio and Video Recording

Images and recordings should only be created where there is a legitimate educational or operational purpose.

Only authorised Academy equipment should normally be used.

Staff must ensure that:

- Appropriate permissions are in place.
- Images are stored securely.
- Images are not retained longer than necessary.
- Images are shared only through authorised systems.

Personal devices should not routinely be used to photograph or record pupils.

Printing and Paper Records

Staff should avoid unnecessary printing of confidential information.

Where printing is necessary:

- Documents should be collected immediately.
- Confidential papers should not be left unattended.
- Secure disposal procedures should be followed.

Paper records remain subject to the same confidentiality requirements as electronic records.

Removable Media

The use of USB memory devices and other removable media presents additional cyber security risks.

Where removable media is authorised:

- It should be encrypted where possible.
- It should be scanned for malware.
- It should contain only necessary information.
- Information should be deleted once no longer required.

Unauthorised removable media must not be connected to Academy systems. BluRock IT will apply proportionate technical restrictions to removable media, including device blocking where the Academy's documented risk assessment requires it, with exceptions authorised, recorded and reviewed.

Cyber Security

Protecting Academy systems is everyone's responsibility.

Staff should:

- Be alert to phishing emails.
- Verify unexpected requests.
- Report suspicious activity immediately.
- Keep passwords secure.
- Lock devices when unattended.
- Install updates when prompted.
- Avoid connecting to unsecured public Wi-Fi when accessing Academy systems.

No member of staff should attempt to investigate suspected cyber incidents independently.

Technical or cyber-security concerns are reported immediately to BluRock IT and the Headteacher. Any concern that may indicate harm to a pupil is also alerted without delay to the DSL or deputy and recorded on CPOMS after immediate protective action. Any suspected personal-data breach is reported immediately to Kathryn McAuley, Data Protection Lead, as well as BluRock IT. The Data Protection Lead records the assessment and determines whether notification to the ICO or affected people is required.

24 Filtering and Monitoring

LCE Academy uses Smoothwall as its confirmed filtering and monitoring provider, in accordance with Keeping Children Safe in Education 2026 and the Department for Education Filtering and Monitoring Standards. BluRock IT provides technical IT support to the Academy but is not the filtering and monitoring provider.

The Academy uses Smoothwall to:

- Filter inappropriate online content.
- Monitor potential safeguarding concerns.
- Support online safety.
- Identify potential cyber security risks.
- Assist with statutory safeguarding responsibilities.

Life Changing Education Ltd retains strategic proprietor responsibility, exercised through Krystian Liptrot as Chair of the proprietor board and company. Sam Gray ensures implementation and is the named senior leader for the filtering and monitoring review. Raheemot Kaffo, DSL, leads safeguarding and online-safety response, supported by DDSLs Lindsey Drews and David Jeal. BluRock IT maintains technical controls, and Smoothwall provides the filtering and monitoring service. The review takes place at least once each academic year and after a material system change, safeguarding incident or identified weakness.

Monitoring information is accessed only by authorised, trained personnel for legitimate safeguarding, security and operational purposes. Immediate or high-risk Smoothwall alerts are reviewed and escalated without delay on the day received. Other safeguarding alerts are reviewed within one school day. Technical alerts are routed promptly to BluRock IT. Safeguarding decisions and outcomes are recorded on CPOMS; technical action is recorded in the IT support system.

The annual review and scheduled checks consider the pupil risk profile, SEND and communication needs, authorised personal-device use, generative AI, and Smoothwall's ability to filter or monitor real-time, dynamic, personalised and AI-generated content. Tests, exceptions and resulting actions are recorded.

25 BluRock IT

BluRock IT provides the Academy's managed IT support service.

Responsibilities include:

- Network management.

- Cyber security.
- Device management.
- User account administration.
- Backup management.
- Software updates.
- Technical support.
- Disaster recovery support.

Where BluRock IT requires access to Academy systems, this will take place under appropriate contractual arrangements and confidentiality obligations.

26 Business Continuity

Technology plays an essential role in maintaining educational provision.

The Academy maintains arrangements to minimise disruption arising from:

- Cyber attacks.
- Network failure.
- Hardware failure.
- Internet outages.
- Cloud service disruption.

Staff should report significant technology issues immediately so that contingency arrangements can be implemented where necessary.

27 Reporting Concerns

Staff should immediately report:

- Lost or stolen devices.
- Suspicious emails.
- Suspected phishing attempts.
- Password compromise.
- Cyber security concerns.
- Inappropriate online behaviour.
- Potential safeguarding concerns arising from technology use.
- Suspected breaches of this policy.

Prompt reporting enables risks to be managed quickly and helps protect the Academy community.

28 Pupil Use of Technology

Technology forms an important part of learning at LCE Academy and pupils are encouraged to develop the knowledge, skills and behaviours required to use digital technology safely, responsibly and effectively.

Pupils will be taught to:

- Use technology respectfully.
- Protect their personal information.
- Recognise online risks.
- Report concerns to trusted adults.
- Respect the privacy of others.
- Think critically about information found online.
- Use digital technology to support learning.
- Understand the opportunities and limitations of Artificial Intelligence.
- Develop positive digital citizenship.

Online safety is embedded throughout the curriculum, including PSHE, computing and pastoral provision.

29 Mobile Phones and Personal Devices

To promote learning, wellbeing and safeguarding, pupils are required to hand in mobile phones and other personal internet-enabled devices at the start of each Academy day.

Devices will be stored securely and returned at the end of the school day unless alternative arrangements have been agreed by the Headteacher.

Pupils must not:

- Use personal devices during the Academy day without permission.
- Photograph or record other pupils or staff.
- Access inappropriate content.
- Attempt to bypass Academy safeguards.
- Use technology to intimidate, bully or harass others.

Any misuse of technology will be managed in line with the Behaviour Policy and, where appropriate, the Safeguarding and Child Protection Policy.

30 Digital Behaviour Expectations

The Academy expects pupils to demonstrate the same standards of behaviour online as they do offline.

This includes:

- Treating others with respect.
- Using appropriate language.
- Respecting copyright and intellectual property.
- Reporting concerns promptly.
- Looking after Academy equipment.
- Following staff instructions.

Where inappropriate online behaviour reflects wider safeguarding concerns, the Academy will respond through a trauma-informed and relational approach whilst taking appropriate action to protect others.

31 Online Safety Education

Online safety education is delivered as a whole-school responsibility.

Learning includes:

- Privacy and personal information.
- Healthy online relationships.
- Cyberbullying.
- Gaming.
- Social media.
- Misinformation and disinformation.
- Artificial Intelligence.
- Online exploitation.
- Radicalisation.
- Financial scams.
- Digital footprints.
- Reporting concerns.

Teaching is adapted to meet pupils' developmental stage, communication needs and individual vulnerabilities.

32 Visitors and Contractors

Visitors and contractors using Academy technology or Wi-Fi must:

- Follow Academy expectations.
- Use systems lawfully.
- Protect confidential information.

- Maintain appropriate cyber security.
- Report security concerns immediately.

Visitor access will normally be restricted to the minimum required for operational purposes.

Temporary accounts may be removed immediately following completion of work.

33

Monitoring Use of Academy Systems

To protect pupils, staff and Academy systems, authorised monitoring of Academy technology may take place.

Monitoring may include:

- Network activity.
- Internet usage.
- Email traffic.
- Filtering alerts.
- Security logs.
- Device management.
- User authentication.
- System performance.

Monitoring is undertaken only where there is a legitimate operational, safeguarding, security or legal purpose.

The Academy will ensure monitoring is proportionate, transparent and compliant with UK GDPR.

34

Misuse of Technology

Examples of unacceptable use include:

- Unauthorised access to Academy systems.
- Sharing passwords.
- Deliberately bypassing filtering systems.
- Downloading unauthorised software.
- Accessing inappropriate material.
- Misusing Artificial Intelligence.
- Unauthorised disclosure of confidential information.
- Cyberbullying.
- Misuse of Academy equipment.
- Using Academy systems for unlawful purposes.

This list is not exhaustive.

35 Responding to Breaches

Where concerns arise, the Academy will respond proportionately.

Responses may include:

- Informal guidance.
- Additional training.
- Removal of system access.
- Investigation.
- Behaviour interventions.
- Disciplinary procedures.
- Referral to external agencies where appropriate.

Where safeguarding concerns are identified, they will be managed in accordance with the Academy's Safeguarding and Child Protection Policy.

36 Cyber Security Incidents

All suspected cyber security incidents must be reported immediately.

Examples include:

- Suspected hacking.
- Malware.
- Phishing attacks.
- Unauthorised access.
- Lost devices.
- Ransomware.
- Unusual system behaviour.

The Academy will work alongside BluRock IT and other specialist providers to investigate, contain and recover from incidents.

Where required, incidents will also be managed in accordance with the Academy's Data Protection Policy and Business Continuity Plan.

37 Training and Professional Development

Digital technology develops rapidly and ongoing professional learning is essential.

Training will include:

- Cyber security.
- Filtering and monitoring.
- Online safeguarding.
- Artificial Intelligence.
- Data protection.
- Password security.
- Safe use of Academy systems.
- Emerging digital risks.

Additional support will be provided where staff roles require enhanced knowledge.

38 Monitoring and Quality Assurance

Implementation of this policy will be monitored through:

- Learning walks.
- IT security audits.
- Filtering and monitoring reviews.
- Device audits.
- Staff feedback.
- Pupil voice.
- Cyber security reviews.
- Data breach reviews.
- Safeguarding audits.
- External IT support reports.

Findings will be used to strengthen digital safety and improve practice across the Academy.

39 Policy Review

This policy will be reviewed:

- Annually in July.
- Following changes to legislation.
- Following significant cyber security incidents.
- Following changes to Academy technology.
- Following updates to Keeping Children Safe in Education 2026.

- Following recommendations from BluRock IT, Kathryn McAuley as Data Protection Lead, any formally appointed independent Data Protection Officer, or an appropriate external authority.

Earlier review may take place where emerging technologies or identified risks require changes to Academy practice.

A Appendix A - Staff Digital Responsibility Checklist

Every member of staff should:

- ☐ Keep passwords secure.
- ☐ Lock devices when unattended.
- ☐ Report suspicious emails.
- ☐ Use Academy email for Academy business.
- ☐ Store information only on approved systems.
- ☐ Record safeguarding concerns on CPOMS.
- ☐ Check recipients before sending confidential information.
- ☐ Keep software updated.
- ☐ Protect Academy devices.
- ☐ Report concerns immediately.

B Appendix B - Artificial Intelligence Checklist

Before using AI, staff should ask:

- Does this improve teaching or administration?
- Have I removed all personal information?
- Have I checked the accuracy of the output?
- Could the content introduce bias?
- Is the information appropriate for pupils?
- Have I applied my own professional judgement before using it?

The member of staff remains responsible for all AI-assisted work.

C Appendix C - Young Person's Internet Policy and Digital Agreement

This appendix is the Academy's Young Person's Internet Policy and Digital Agreement. It must be explained in an age-respectful, communication-friendly way and adapted where a pupil needs visuals, symbols, additional processing time or SaLT support. Pupils have the right to safe, accessible technology, clear explanations of filtering and monitoring, privacy that is respected within safeguarding and legal limits, and prompt help when something online worries or harms them.

Pupils may report a concern to any trusted adult, their form tutor, Liv Williams, Ben Corless or the safeguarding team. Staff will listen without blame, preserve evidence safely, avoid unnecessarily viewing or forwarding harmful or illegal content, and follow safeguarding procedures. Responses to unsafe or unacceptable use will be supportive, educational and proportionate under the Behaviour Policy; safeguarding action takes priority where a pupil may be at risk.

Pupils are expected to:

- Respect Academy technology.
- Follow staff instructions.
- Protect passwords where applicable.
- Treat others respectfully online.
- Report concerns immediately.
- Use technology to support learning.
- Avoid accessing inappropriate content.
- Hand in mobile phones at the start of the Academy day.

Failure to meet these expectations will be addressed through the Academy's Behaviour Policy.

D Appendix D - Remote Working Checklist

Before working remotely, staff should ensure:

- ☐ Devices are secure.
- ☐ Confidential information cannot be overlooked.
- ☐ Academy systems are accessed using approved methods.
- ☐ Passwords remain confidential.
- ☐ Printed documents are stored securely.
- ☐ Devices are locked when unattended.

☐ Confidential waste is disposed of appropriately.

E Appendix E - Policy Summary

LCE Academy believes that technology should enhance learning, strengthen safeguarding and improve operational effectiveness.

Every member of the Academy community has a responsibility to use digital technology safely, responsibly and professionally.

Through effective leadership, robust cyber security, clear expectations and ongoing education, the Academy seeks to create a digital environment that supports learning while protecting the safety, privacy and wellbeing of all members of the Academy community.