



Online Safety Policy

1. Purpose

NewHeart Learning Limited is committed to ensuring that pupils, staff, volunteers, visitors and other users are protected from risks associated with technology, including the internet, mobile devices, online platforms and digital communications. This policy provides clear guidance to safeguard everyone within the provision and promote safe, responsible and professional online behaviour.

2. Scope

This policy applies to:

- all pupils, employees, volunteers, contractors and visitors using NewHeart Learning devices, networks or online services;
- personal devices used on NewHeart premises or used to access NewHeart systems, information or communications;
- online communications, platforms, software and cloud services used for learning, administration or NewHeart business; and
- remote or off-site use of technology where the activity is connected with NewHeart Learning.

3. Roles and Responsibilities

3.1 Online Safety Lead / DSL

Daniella Hart, Designated Safeguarding Lead, is the lead for online safety and will oversee implementation of this policy, provide or arrange appropriate guidance and training, and respond to online-safety concerns and incidents.

3.2 All Staff and Volunteers

- promote safe and responsible use of technology;
 - model appropriate professional online behaviour;
 - follow the Staff Acceptable Use Agreement at Appendix 2;
 - report online-safety, safeguarding, cyber-security and data-protection concerns promptly;
- and
- support pupils to understand and manage online risks.

3.3 Pupils

- use NewHeart technology responsibly;
- follow the Pupil Online Safety Agreement;
- report inappropriate, unsafe or upsetting online content or behaviour to a member of staff.

3.4 Parents and Carers

- support NewHeart's online-safety guidance;
- discuss the Pupil Online Safety Agreement with their child;
- report relevant online-safety concerns affecting their child.

4. Acceptable Use

NewHeart devices, systems and accounts are provided primarily for educational, safeguarding and legitimate business purposes. Limited reasonable personal use by employees may be permitted where it does not interfere with work, create risk, breach confidentiality or contravene this policy.

- Users must not access, create, store or share illegal, discriminatory, abusive, sexually inappropriate or otherwise harmful material.
- Passwords must be strong, kept confidential and never shared. Multi-factor authentication must be used where NewHeart requires it.
- Users must not attempt to bypass filtering, monitoring, security controls or access restrictions.
- Only authorised software, applications, platforms and cloud services may be used for NewHeart business or pupil information.
- Suspected phishing, malware, compromised accounts or other cyber-security incidents must be reported immediately.

Mobile Phones and Personal Smart Devices

Pupil use of mobile phones and personal smart devices during the provision day is governed by NewHeart Learning's Behaviour Policy and Mobile Phones, Smart Devices and Earbuds procedures. NewHeart operates as a mobile phone-free provision by default, subject to agreed reasonable adjustments and exceptional circumstances.

5. Education and Training

- Online-safety education will be embedded within learning and pastoral work where appropriate to pupils' needs.
- Staff will receive appropriate safeguarding and online-safety training and updates.
- NewHeart will provide or signpost parents/carers to relevant guidance where appropriate.
- Staff will be made aware of filtering and monitoring expectations and their responsibility to report concerns.

6. Managing Risks

6.1 Filtering and Monitoring

NewHeart Learning will use appropriate filtering and monitoring arrangements to reduce access to harmful or inappropriate content and to support safeguarding. Filtering and monitoring do not replace staff supervision, professional curiosity or the need to report concerns.

Use of NewHeart systems may be logged or monitored for safeguarding, security, compliance and legitimate business purposes, subject to applicable law and NewHeart's privacy and data-protection arrangements.

Filtering and monitoring will be undertaken in accordance with NewHeart Learning's data-protection arrangements and relevant privacy notices. Appropriate data-protection impact assessments will be undertaken where required when new monitoring technologies are introduced or significantly changed.

NewHeart Learning will review its filtering and monitoring arrangements at least annually, and sooner where significant changes in technology, systems or identified risks require this. The review

will consider the specific needs and risk profile of NewHeart pupils, including age, SEND and vulnerability.

NewHeart will also consider the risks presented by real-time, dynamic, personalised and AI-generated content when assessing whether its filtering and monitoring arrangements remain appropriate and effective.

Responsibility for filtering and monitoring will be clearly allocated between senior leadership, the DSL/Online Safety Lead and relevant IT support. Significant concerns, identified gaps and actions arising from filtering and monitoring reviews will be recorded and followed up appropriately.

6.2 Cyberbullying, Harassment and Harmful Content

Online bullying, harassment, discriminatory abuse, sexual harassment, threatening communications and other harmful online behaviour are prohibited. Incidents involving pupils will be addressed under safeguarding and behaviour procedures. Employee conduct may also be addressed under the Staff Code of Conduct, Anti-Bullying/Harassment arrangements and Disciplinary Policy.

6.3 Data Protection and Confidentiality

Personal data must be handled in accordance with NewHeart's Data Protection and Staff Confidentiality requirements. Pupil, family and staff information must only be accessed, used, shared and retained for legitimate authorised purposes.

7. Reporting and Responding to Incidents

- Staff personal devices must not be used to photograph, film or audio-record pupils unless expressly authorised for a legitimate NewHeart purpose and in accordance with safeguarding and consent arrangements.
- Pupil images, videos, safeguarding information, EHCP information, assessment information or other confidential records must not be stored on personal devices.
- Personal mobile-phone use during working time must be reasonable and must not interfere with supervision, safeguarding or professional duties.
- Staff must not use personal phone numbers or personal social-media accounts to communicate privately with pupils.
- Any lost or stolen device that may contain or provide access to NewHeart information must be reported immediately.

8. Email, Messaging and Online Communication

- NewHeart business should be conducted through approved NewHeart accounts and systems wherever these are provided.
- Confidential or identifiable pupil information must not be sent to personal email accounts or stored in personal cloud accounts.
- Staff communications with pupils and parents/carers must remain professional, appropriate and capable of organisational oversight.
- Staff must not engage in private or secret online communications with pupils.
- Group messaging or services such as WhatsApp must only be used for NewHeart business where specifically authorised and appropriate safeguards are in place.

9. Artificial Intelligence (AI) Tools

AI tools may only be used for NewHeart work where their use is appropriate, lawful and consistent with NewHeart's safeguarding, confidentiality and data-protection requirements.

Before introducing a new AI product or service for pupil-facing use, NewHeart will consider its safeguarding, data-protection, age-appropriateness, filtering and monitoring arrangements and relevant DfE AI product-safety standards.

- Identifiable or confidential information about pupils, families, employees or safeguarding matters must not be entered into unapproved public AI systems.
- Staff must not rely on AI-generated content without checking it for accuracy, suitability, bias and safeguarding implications.
- AI must not be used as the sole basis for decisions about a pupil or employee where the decision requires professional judgement or may have a significant impact on the individual. Appropriate human oversight and professional judgement must always be maintained.
- Any AI-generated material used for NewHeart purposes remains the responsibility of the employee using it.

Pupil use of AI

Pupils may only use generative AI tools as part of NewHeart Learning activities where the tool and proposed use have been approved by NewHeart and appropriate safeguards are in place. Staff must consider the pupil's age, developmental needs, SEND, safeguarding needs and the age restrictions and terms applicable to the AI service.

Where pupils use AI as part of learning, appropriate staff supervision and filtering/monitoring arrangements must be in place. Pupils will be supported to understand that AI-generated information may be inaccurate, misleading, biased or inappropriate and should not automatically be treated as factual.

10. Remote Learning and Online Meetings

- Online teaching or meeting platforms used with pupils must be approved by NewHeart.
- Staff and pupils must maintain professional and safe communication practices.
- Online interactions with pupils should take place through authorised accounts and arrangements.
- Recording of online sessions must only take place where specifically authorised and where safeguarding, consent and data-protection requirements have been considered.

11. Reporting and Responding to Incidents

Online-safety incidents and safeguarding concerns must be reported promptly to the DSL/Online Safety Lead. Data breaches and cyber-security incidents must also be reported promptly to the appropriate NewHeart manager.

Incidents will be recorded, assessed and responded to proportionately. This may include contact with parents/carers, commissioners, the local authority, police, social care, LADO, the data-protection lead or other external agencies where appropriate.

12. Staff Breaches of this Policy

A breach of this policy or the Staff Acceptable Use Agreement may result in restricted access to NewHeart systems, additional training or management action. Serious or repeated breaches may be dealt with under NewHeart's Disciplinary Policy and Procedure and, where relevant, safeguarding or external referral procedures.

13. Related Policies and Procedures

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection and Staff Confidentiality Policy
- Anti-Bullying, Harassment and Sexual Harassment Policy
- Disciplinary Policy and Procedure
- Whistleblowing Policy

14. Monitoring and Review

This policy will be reviewed annually, or sooner where there are significant changes in technology, legislation, safeguarding guidance, filtering/monitoring arrangements or NewHeart's operating practices.

NewHeart will consider the effectiveness of its online-safety education, staff training, reporting procedures and technical safeguards as part of the review.

Date of last review:	11 August 2026
Date to review:	11 August 2027
Author:	Daniella Hart Head of Provision
Signed:	<i>Daniella Hart</i>

Appendix 1 - Pupil and Parent/Carer Online Safety Agreement

NewHeart Learning recognises the importance of children and young people being able to use the internet for learning, personal development and social engagement, including social media, games and apps. We aim to support pupils to use these tools safely and responsibly while maintaining appropriate safeguards.

Pupils and parents/carers should read and discuss this agreement as part of induction.

Pupil Agreement

I understand that:

- I am responsible for my behaviour when using the internet, including social media, games and apps, and for the content I access and share.
- I will not intentionally browse, download or upload material that is offensive, inappropriate or illegal. If I encounter such material accidentally, I will report it to a member of staff.
- I will not send threatening, bullying, offensive or illegal content to anyone.
- I will keep personal information private and will not share passwords.
- I will not arrange to meet someone I only know online without discussing it with my parent/carers and a trusted adult.
- If something online upsets or worries me, or I receive concerning messages, I can speak to any member of NewHeart staff.
- I will only use AI tools at NewHeart when a member of staff has said I can use them.
- I understand that AI can sometimes give incorrect, misleading or inappropriate information, and I will ask a member of staff if I am unsure about something it produces.
- I understand that my use of NewHeart internet and systems may be monitored and logged to help keep people safe.
- I understand that if I do not follow these rules, my parent/carers may be contacted and NewHeart may take appropriate action.

Pupil name / signature	
Parent/Carer signature	
Date	

Appendix 2 - Staff IT, Email, Internet & Acceptable Use Agreement

This agreement applies to all NewHeart Learning employees and should be read alongside the Online Safety & Acceptable Use Policy, Staff Code of Conduct, Safeguarding Policy and Data Protection/Confidentiality requirements.

By signing this agreement, I confirm that I will:

- use NewHeart devices, networks, email accounts and systems responsibly, professionally and primarily for legitimate NewHeart purposes;
- keep passwords and authentication details secure, use multi-factor authentication where required, and never allow another person to use my account;
- lock my screen or secure my device whenever it is left unattended;
- use only authorised software, applications, storage and cloud services for NewHeart information;
- not deliberately access, create, download, store or share illegal, offensive, discriminatory, sexually inappropriate or harmful material;
- not attempt to disable or bypass NewHeart filtering, monitoring, security or access controls;
- report phishing, suspicious emails, malware, compromised passwords, lost devices, accidental disclosures and suspected data breaches immediately;
- use NewHeart email/accounts rather than personal email/accounts for confidential NewHeart business wherever NewHeart accounts are provided;
- never send or forward confidential or identifiable pupil information to my personal email address or personal cloud storage;
- not store pupil records, EHCPs, safeguarding information, photographs, videos or other confidential NewHeart data on my personal device;
- not photograph, film or record pupils on a personal device unless expressly authorised under a specific NewHeart arrangement;
- keep communications with pupils and parents/carers professional and use approved communication channels;
- not add, follow or privately message current pupils through personal social-media accounts, and maintain appropriate professional boundaries online;
- only use WhatsApp or similar messaging services for NewHeart business where NewHeart has specifically authorised the arrangement;
- not enter identifiable or confidential pupil, family, employee or safeguarding information into public or unapproved AI tools;
- check the accuracy, appropriateness and safeguarding implications of any AI-generated material before using it for NewHeart purposes;
- respect copyright, intellectual-property and software-licensing requirements;
- understand that NewHeart may monitor or log use of its systems for safeguarding, security, compliance and legitimate business purposes, subject to applicable law;
- return NewHeart devices and information when requested or when my employment ends and not retain copies of confidential NewHeart information; and
- report any online-safety or safeguarding concern promptly to the DSL.

I understand that failure to comply with this agreement may result in access to NewHeart systems being restricted and may lead to management or disciplinary action. Serious concerns may also be dealt with under safeguarding procedures or referred to an appropriate external body where required.

Employee name	
Job title	
Employee signature	
Date	
Manager / induction check	