Highcroft School

Online Safety, Cyber Security and Acceptable Use Policy

Copyright – to be used only with prior and express permission of Keys Group.

Online Safety, Cyber Security and Acceptable Use Policy

Policy Number:	EDU.POL.009	Policy Owner Job Role	Quality Manager
Issue Number:		Ratified By	Quality Director
Issue Date:	01.07.26	Service Type:	Schools
		Applicable Services:	Education
Contributors	Rob Arrowsmith		
Mandatory Policy	Yes		
Note	This policy must not be amended without prior approval of the Education Director		

Table of Contents

Section	
1	**Supporting Documents**
2	**Introduction**
3	**Aim & Scope**
4	**Abbreviations/Definitions**
5	**Policy Content**
6	**Responsibilities**
7	**Training Requirements**
8	**Equality Impact Statement**
9	**Sources of Information / References**
10	**Version Control (where else is this policy located, ie. Circle, Nourish, Radar)**
11	**Appendices**

1. Supporting Documents

- Safeguarding Children in Education Policy (EDE.POL.002)
- Mobile Phone Policy (EDU.POL.040)
- Data Protection Policy
- Behaviour Policy (EDU.POL.027) and Anti-bullying Policy
- Searching, Screening and Confiscation Policy (EDU.POL.035)

Related policies are held within RADAR in the School's policy folder.

2. Introduction

At Highcroft School, we want every pupil to benefit from technology while staying safe online. Many of our pupils are more vulnerable to online harm because of their experiences and needs, so we protect them with strong filtering and monitoring, clear rules for using technology, and education that builds their resilience. We treat online safety as part of safeguarding, not as a separate technical matter.

Copyright – to be used only with prior and express permission of Keys Group.

This policy sets out how we keep pupils and staff safe online, how we filter and monitor our systems, how we expect technology to be used, how we manage generative AI and cyber security, and how we respond to online incidents.

3. Aim & Scope

This policy applies to all staff, governors, pupils, parents and carers, volunteers and visitors at Highcroft School, and to all use of our IT systems, networks and devices, on and off site. It aims to:

- Protect pupils and staff from online harm and treat online safety as a safeguarding matter.
- Set out how we filter and monitor our systems and review them effectively.
- Make clear how technology must be used by pupils, staff, volunteers and visitors.
- Set our approach to generative AI, deepfakes and cyber security.
- Explain how we educate pupils and how we respond to and record online incidents.

4. Abbreviations and Definitions

The 4Cs. The four areas of online risk: content (harmful material), contact (harmful interaction with others), conduct (a pupil's own or others' harmful behaviour) and commerce (financial harm such as scams, gambling or fraud).

Filtering. Technology that blocks access to harmful and inappropriate online content on our systems and devices.

Monitoring. The means by which we identify when a user accesses or searches for harmful content, so that staff can respond.

Generative AI. Tools that create text, images, audio or video. A deepfake is AI-generated or AI-altered content that shows a real person doing or saying something they did not.

5. Policy Content

5.1 Principles and Approach

Our approach rests on the following principles.

Online safety is safeguarding. We respond to online risk with the same seriousness as any other safeguarding concern.

Filter, monitor and review. We block harmful content, we monitor for risk, and we check that our systems work and record those checks.

Staff as well as pupils. Our rules and our monitoring cover staff use of our systems and accounts, not only pupils.

Educate and empower. We teach pupils to recognise risk, behave well online and ask for help, in a way that is accessible to them.

Copyright – to be used only with prior and express permission of Keys Group.

Plan for new technology. We keep pace with generative AI, deepfakes and new platforms, and we update our practice.

Security by design. We protect our systems and data against cyber threats, and we train our people to do the same.

5.2 Online Safety, Cyber Security and Acceptable Use in Practice

The risks we manage

We manage online risk across the 4Cs: content, such as harmful, extremist, self-harm or pornographic material and misinformation; contact, such as grooming, peer pressure and exploitation; conduct, such as cyberbullying, sharing of intimate images and misuse of social media; and commerce, such as scams, fraud and gambling. We pay particular attention to the heightened risks for our pupils.

Filtering and monitoring

At Highcroft School, we provide appropriate filtering and monitoring on all our internet-connected devices and networks. We assign clear roles for managing these systems, we block harmful and inappropriate content without unreasonably getting in the way of learning, and we have monitoring in place that meets our safeguarding needs. We review the effectiveness of our filtering and monitoring at least once every academic year, and more often if needed. The review includes checks that filtering is working on all internet-connected devices in all relevant locations, and we keep a record of these checks. We record this annual review using the Keys filtering and monitoring checklist, the White Book, which is completed by the senior leadership team, the designated safeguarding lead, the IT service provider and the responsible governor. Our filtering and monitoring is informed by our Prevent duty risk assessment, and we use the DfE filtering and monitoring standards and self-assessment service. Staff know how to escalate a concern the moment monitoring identifies one.

Acceptable use of technology

Everyone who uses our systems agrees to use them safely and responsibly. Pupils follow the acceptable use agreement at Appendix B. Staff, volunteers, governors and visitors follow the agreement at Appendix C, which covers the use of school accounts and devices, the handling of data, professional conduct online, and the use of personal devices. Our monitoring covers staff use of our systems and accounts as well as pupils'. The use of mobile phones is managed through our Mobile Phone Policy (EDU.POL.040).

Online safety education

We teach online safety through the curriculum, including relationships, sex and health education, computing and bespoke work, in a way that is accessible to pupils with special educational needs and complex needs. Pupils learn to

Copyright – to be used only with prior and express permission of Keys Group.

recognise risk, behave respectfully online, protect their personal information, and report concerns, and we help them build digital resilience.

Generative AI and deepfakes

Where we use generative AI, we use it safely and in line with DfE guidance, protecting personal data and intellectual property and checking AI output. We teach pupils about the risks of AI, including misinformation and AI-generated content. We treat the creation or sharing of AI-generated or altered sexual images of a child, including deepfakes, as a form of child-on-child abuse and a safeguarding matter, and we respond through our Safeguarding Policy (EDE.POL.002).

Cyber security

We protect our systems and data against cyber threats in line with the DfE cyber security standards. This includes strong passwords and multi-factor authentication, regular backups, keeping systems up to date, controlling access to data, and guarding against phishing. All staff receive cyber security training at least once a year, and a governor takes responsibility for cyber security. We have a plan for responding to and reporting a cyber incident, and we treat the loss of personal data as a matter for our Data Protection Policy.

Critical systems, pupil safeguarding data and backup arrangements will be tested periodically as part of the school's cyber resilience programme.

Managing and reporting online incidents

We respond to online incidents quickly and proportionately. Cyberbullying and harmful online conduct are dealt with through our Behaviour and Anti-bullying policies. Where an electronic device needs to be searched, we follow our Searching, Screening and Confiscation Policy (EDU.POL.035), and a suspected indecent image of a child is never viewed and is referred to the designated safeguarding lead. We record online safety incidents on CPOMS, act on safeguarding concerns through our Safeguarding Policy (EDE.POL.002), and involve the police and other agencies where needed.

5.3 Recording, Monitoring and Reporting

Online safety incidents are recorded on CPOMS, and the records of our filtering and monitoring checks are kept in the Keys filtering and monitoring checklist, the White Book, and are available for review. Leadership and governors review online safety and filtering and monitoring at least once a year, so that Highcroft School keeps its systems and practice effective.

5.4 Equality and Inclusion

At Highcroft School, this policy is applied fairly and in line with the Equality Act 2010. We make reasonable adjustments so that pupils with special educational needs and disabilities can use technology safely, while keeping the same

Copyright – to be used only with prior and express permission of Keys Group.

protections in place for them. Any concern that this policy disadvantages a pupil should be raised with the headteacher.

6. Responsibilities

6.1 Pupils

Use technology safely and respectfully, follow the acceptable use agreement, and report anything that worries them.

6.2 Staff and volunteers

Follow the staff acceptable use agreement, model safe use, supervise pupils online, and report concerns promptly.

6.3 Leadership

Leadership at Highcroft School makes sure this policy works in practice, that filtering and monitoring are effective and reviewed, and that staff and pupils are trained.

6.4 Governance

The proprietor and governors at Highcroft School make sure the school meets its filtering, monitoring and cyber security duties and review them at least once a year. The named governor with responsibility for online safety and cyber security at Highcroft School is David Joy.

6.5 Designated safeguarding lead

Leads on online safety incidents and oversees filtering and monitoring with the IT and filtering and monitoring team.

6.6 Filtering and monitoring team

The roles for managing filtering and monitoring at Highcroft School are assigned to Christine Wade and Stephanie Goddard, who keep the systems effective, carry out and record the reviews, and escalate concerns.

6.7 Parents and carers

Support the school's online safety rules and reinforce safe online behaviour at home.

6.8 Named leads

The designated safeguarding lead at Highcroft School is Stephanie Goddard.

7. Training Requirements

All staff receive online safety training at induction and regular updates, including the filtering and monitoring roles and how to escalate concerns. All staff receive cyber security training at least once a year, and a governor receives cyber security

Copyright – to be used only with prior and express permission of Keys Group.

training for their oversight role. The designated safeguarding lead and the filtering and monitoring team at Highcroft School receive role-specific training.

8. Equality Impact Statement

All policies will be developed and implemented in a manner that promotes equality, diversity, and inclusion, ensuring fair and equitable treatment for all individuals. Policies must align with relevant equality legislation and reflect the expectations and standards set by our regulatory bodies. They will demonstrate a commitment to eliminating discrimination, advancing equality of opportunity, and fostering an inclusive environment that respects and values the diverse needs, backgrounds, and experiences of those we support, as well as our workforce.

9. Sources of Information / References

This policy reflects current statutory guidance and legislation, including:

- Keeping Children Safe in Education (DfE, 2025, and 2026 from 1 September 2026), including filtering and monitoring, the 4Cs and generative AI.
- Meeting digital and technology standards in schools and colleges (DfE), including the filtering and monitoring standards and the cyber security standards.
- Online Safety Act 2023.
- Generative artificial intelligence in education (DfE).
- The Prevent duty, whose risk assessment informs our filtering and monitoring.
- Data Protection Act 2018 and UK GDPR, applied through our Data Protection Policy.
- Education Act 1996 and Equality Act 2010.

10. Version Control

This document can also be found in Radar. This policy is reviewed annually, or sooner if legislation or statutory guidance changes. The next review date and version history are recorded in the control table above. The named owner for review at Highcroft School is the headteacher.

11. Appendices

Copyright – to be used only with prior and express permission of Keys Group.

11.1 Appendix A: School-Specific Annex

At Highcroft School the following local arrangements apply:

- Filtering and monitoring systems and provider: Securus
- Filtering and monitoring lead and team: Christine Wade, Pastoral Lead and Stephanie Goddard, Headteacher.
- Named governor for online safety and cyber security: David Joy.
- Where the completed filtering and monitoring review (White Book) is held:
- Designated safeguarding lead: Stephanie Goddard

Copyright – to be used only with prior and express permission of Keys Group.

11.2 Appendix B: Pupil Acceptable Use Agreement

This agreement is shared with pupils in language suited to their age and understanding.

Primary and younger pupils. When I use the school's computers, tablets or other technology, I will: ask a member of staff before I use them; only use websites and apps I am allowed to; keep my password safe; be kind to others online; tell a member of staff if I see anything that upsets or worries me; and look after the equipment.

Secondary and older pupils. When I use the school's IT systems and the internet, I will: use them responsibly and mainly for learning; keep my passwords secret and not use anyone else's account; not try to get around the school's filtering; not share personal information or other people's images without permission; be respectful and never bully or harass anyone online; not create or share sexual or abusive images, including AI-generated or altered ones; and report anything inappropriate or upsetting to a member of staff.

Parent and carer agreement. I will support my child to understand and follow these rules and encourage safe and responsible use of technology at home.

Copyright – to be used only with prior and express permission of Keys Group.

11.3 Appendix C: Staff, Governor and Visitor Acceptable Use Agreement

When I use the school's IT systems, accounts and devices, I will: use them lawfully, professionally and mainly for my work; keep my login details secure and use multi-factor authentication where it is in place; protect personal and sensitive data and follow the Data Protection Policy; not access, store or share inappropriate material; report any online safety or cyber security concern, and any suspected data breach, without delay; never attempt to view a suspected indecent image of a child but refer it to the designated safeguarding lead; model safe and respectful online behaviour; and follow the rules on personal devices and on communicating with pupils. I understand that my use of the school's systems and accounts is monitored.

Staff must not use personal messaging applications to communicate with pupils unless authorised by school procedures.

Copyright – to be used only with prior and express permission of Keys Group.