Huxlow Academy

Ambition • Respect • Pride

Policy Owner	Department	Effective Date	Approval Date	Review Cycle	Revision Due Date
Zoë Correa	Safeguarding	March 2026	Mar 2026	Annually	Mar 2027

Online Safety Policy

Policy Approver: Local Governing Board

Version Control

Version Number	Date of Change	Changes Made
1	March 2026	All changes made in red

Huxlow Academy

Ambition • Respect • Pride

Contents

1. Policy Name

Online Safety Policy

2. Policy Aims

Huxlow Academy aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

3. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy is based on and complies with the following statutory and advisory guidance:

- Keeping Children Safe in Education (KCSIE 2025)
- DfE Preventing and Tackling Bullying (2024)
- DfE Teaching Online Safety in Schools
- DfE Searching, Screening and Confiscation (2022)
- DfE Cyberbullying: Advice for Headteachers and School Staff (2014)
- DfE Sexual Violence and Sexual Harassment Guidance (2021)
- UKCIS "Sharing nudes and semi-nudes" (2020)
- Prevent Duty guidance on protecting children from radicalisation

This policy also reflects the following legislation:

- Online Safety Act 2023 (duties relating to harmful online content)
- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 (powers to search, seize, delete)
- Equality Act 2010
- Children Act 1989 and Children Act 2004 (safeguarding duties)
- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Public Order Act 1986
- Working Together to Safeguard Children (2023)

4. Roles and Responsibilities

4.1 The Local Governing Board

The Local Governing Board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Local Governing Board will coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The Local Governing Board governor who oversees online safety is Richard Glasspool.

All Local Governing Board governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix C)

4.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the academy.

4.3 The Designated Safeguarding Lead

Details of the academy's DSL and Deputy DSL are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DDSL takes lead responsibility for online safety in academy, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix D) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the behaviour for life policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

4.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at college, including terrorist and extremist material
- Ensuring that the academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the academy's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix D) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour for life policy

4.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix C), and ensuring that students follow the school's terms on acceptable use (appendices B and C)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix D) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy behaviour for life policy

4.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the academy's ICT systems and internet (appendices B)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- Safer Internet - https://saferinternet.org.uk/guide-and-resource/parents-and-carers
- Childnet International - https://www.childnet.com/parents-and-carers/
- Healthy relationships – www.gov.uk/government/collections/disrespect-nobody-campaign

4.7 Visitors and members of the community

Visitors and members of the community who use the academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix C).

5. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

From September 2020 **all** schools have to teach:

- Relationships and sex education and health education in secondary schools
  This new requirement includes aspects about online safety.

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact, conduct and commerce, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, they will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- The safe use of social media and the internet will also be covered in other subjects where relevant.
- What positive, healthy and respectful online relationships look like
- The effects of their online actions on others
- How to recognise and display respectful behaviour online
- Where to go for help and support when they have concerns about content or contact on the internet or other technologies
- Freedom of speech
- The role and responsibility of the media in informing and sharing public opinion
- The concept of democracy, freedom, rights and responsibilities

The academy will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating parents about online safety

The academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or social media accounts. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyberbullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti-bullying policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know

how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PSHE education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The academy also sends links on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the academy antibullying policy. Where illegal, inappropriate or harmful material has been spread among students, the academy will use all reasonable endeavours to ensure the incident is contained.

The DSL/DDSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

Mobile devices, including smart watches, are not permitted on the academy site. Where students bring mobiles devices onto the academy site, academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads, other tablet devices and smart watches, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of college discipline), and/or
- Report it to the police

Any search will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

8. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the academy's ICT systems and the internet. Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

9. Students using mobile devices in school

It is acknowledged that for the purposes of track and trace, students may bring their devices to school. These are not to be seen or heard on the academy premises. If a student is found to be in possession of a mobile device, this will be confiscated and the student will have an after-school detention (Reset), the day after. The student can collect their mobile device from Reception at the end of the school day.

10. Staff using work devices outside of school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the academy's terms of acceptable use.

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Not sharing their password with others
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates
- Any USB devices containing data relating to the academy must be encrypted

Staff members must not use the device in any way which would violate the academy's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Robust processes are in place for staff to return academy IT equipment before they cease to be employed by the academy.

11. How the academy will respond to incidents of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The network manager logs behaviour and safeguarding issues related to online safety in secure area on Google Teams and on CPOMS where Smoothwall automatically logs concerns that the filter captures.

This policy will be reviewed bi-annually by the Assistant Headteacher/ Deputy Designated Safeguarding Lead. At every review, the policy will be shared with the Local Governing Board.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Antibullying policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Signed:.....D McVean.....
Chair of Local Governing Board

Date: .....25.03.2026.....