



# The Hinckley SCHOOL

## E-Safety Policy 2025-26

<b>Date of last review:</b>	<b>August 2025</b>
<b>Reviewed by:</b>	<b>Kate Priestnall, Director of Student Welfare and DSL Peter Harrison, IT Manager</b>
<b>Approved by Governors:</b>	<b>October 2025</b>
<b>Frequency of review:</b>	<b>Annually</b>
<b>Date of next review:</b>	<b>August 2026</b>

## Contents

1. Rationale	Page 3
2. Principles	Page 4
3. Information Systems and Security	Page 4
I.    Web filtering and monitoring	Page 5
II.   Computer Activity	Page 5
III.  Email	Page 5
IV.  Assessing Risk	Page 6
4. Reporting and Responding to incidents of Misuse	Page 6
5. Use of Digital and Video Images	Page 6
6. Social Media – Protecting Professional Identity	Page 7
7. Artificial Intelligence	Page 7
8. Personal data	Page 7
9. Roles and Responsibilities	Page 8
Appendix - ICT Acceptable Use Policy for Students	Page 10
Online Safety during Remote Learning	Page 12

## 1. Rationale

### What do we mean by E-Safety?

E-Safety is about safe and responsible use of modern technology to include:

- existing and future stationary/mobile electronic devices;
- existing and developing Internet-based technologies, used for the purposes of learning, business and recreation.

The Futures Trust and all schools within the Trust believes a clear e-safety policy, consistently and fairly applied, underpins effective education. The use of the internet and connected devices pose a risk to the safety of the young people in our care. The Trust will make clear to all school staff, students and parents the high standards of behaviour expected at all times.

The Hinckley School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within the school, while supporting staff and students to identify and manage risks independently and with confidence. Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the schools' e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. E-safety will be a focus in all areas of the curriculum and staff should take active steps to reinforce e-safety messages across the curriculum.

Keeping Children Safe in Education 2025 has included changes to their list of content risks under online safety and have added disinformation, misinformation and conspiracy theories as online harms.

This e-safety policy should be read alongside other relevant school policies, including:

- Safeguarding and Child Protection
- Guidance for Safety Working Practice
- Dealing with Allegations of Abuse Against Staff and Volunteers

- Whistleblowing Policy
- Acceptable Use Policy
- Behaviour Policy

## **2. Principles**

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of the school's ICT systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Heads of Schools, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school but are linked to membership of the school.

The school will deal with such incidents within this policy, and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school. In order to safeguard our community external agencies including the Police may also become involved.

## **3. Information Systems and Security**

The security of the school's information systems, and users, will be reviewed regularly and as follows:

- Virus and malware protection is updated continually;
- School computer activity will be monitored through Securus (monitoring and alerting is provided by Warwickshire County Council Digital Safeguarding Service). Any concerns identified by this service are passed to the school Designated Safeguarding Leads for further investigation
- Students and staff are not able to download or access software that has not been authorised and approved by the school IT Services team.
- The network manager is notified immediately of any Internet access concerns by the on-premise Smoothwall web filter. These concerns are reviewed and passed to the DSL (Designated Safeguarding Lead) where appropriate.
- Files held on the school's network will be continually checked for viruses and other malware;
- The network manager will regularly review the security of the school network and identify areas where threat mitigations can be enhanced. This will include the monitoring of relevant software updates on all network devices.
- The Futures Trust has employed the services of an external company to provide MDR (Managed Detection and Response) to provide proactive protection from cyberthreats, using

advanced detection and rapid incident response. The MDR supports the school by providing a combination of technology and human expertise to perform cyberthreat hunting, monitoring and response.

#### I. Web Filtering and Monitoring

The Trust will work with all schools to ensure that systems to protect students are reviewed and improved. The network manager will regularly review and update filtering systems as required. If staff or students discover unsuitable sites, the URL must be reported to IT Services immediately. The school's broadband access is monitored and filtered by Smoothwall. Regular updates to this platform are carried out by the network manager and filtering categories and blocklists are updated regularly as provided by Smoothwall. The level of filtering applied is appropriate to the age and maturity of students, with different filtering policies in place for KS3, KS4, KS5 Students, and staff. The school's filtering policy meets the [DfE Filtering and monitoring Standards for Schools and Colleges](#). Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal will be reported to appropriate agencies such as IWF or CEOP.

The network manager will carry out half-termly testing of web filtering policies using a tool provided by SWGfL and the UK Safer Internet Centre ([www.testfiltering.com](http://www.testfiltering.com)) to ensure that students are adequately protected from harmful, illegal and inappropriate content.

#### II. Computer Activity

All school computers have Securus software installed. The purpose of Securus is to enable the School to enforce its own Acceptable Use Policy (AUP) and control misuse of computing resources. Securus flags inappropriate activity and these reports are analysed by the Warwickshire County Council Digital Safeguarding Service before being passed to the school DSLs for further investigation. The software is able to monitor keyboard input and the content of the screen including web pages and documents. There is also an AUP (Acceptable Use Policy) which is displayed before any user may gain access to the computer.

#### III. Email

Email usage and accounts will be monitored closely to reflect the school's high standards:

- Students may only use approved email accounts;
- Students must immediately tell a teacher if they receive offensive email;
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult;
- Excessive social email use can interfere with learning and will be restricted;
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper;

- Staff should only use school email accounts to communicate with students as approved by the Senior Leadership Team;
- Staff should not use personal email accounts during school hours or for professional purposes.

#### IV. Assessing Risk

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly.

#### **4. Reporting and Responding to Incidents of Misuse**

The staff and student AUP set out the requirements in relation to the reporting of unsuitable or inappropriate activities. Where such activities also raise a safeguarding concern, the school's Child Protection and Safeguarding Policy and relevant procedures will be followed.

It is more likely that the school will need to deal with incidents that involve inappropriate, rather than illegal, misuse. Incidents will be dealt with as soon as possible in a proportionate manner and members of the school community will be made aware that incidents have been dealt with. Incidents of misuse will be dealt with through normal behaviour and disciplinary procedures.

#### **5. Use of Digital and Video Images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying and/or exploitation to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is increasingly common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

Parents and Carers can opt out of their child's image being used digitally in school.

## **6. Social Media – Protecting Professional Identity**

The AUP sets out the expectations about the appropriate use of social media by staff, students and parents/carers. This guidance must be followed in order to ensure that staff, students and parents/carers do not engage in any activity which may cause them to breach acceptable standards of conduct.

## **7. Artificial Intelligence (AI)**

Artificial Intelligence (AI) tools are becoming commonplace and ever more capable. Elements of AI are currently being integrated into many software packages and websites. Only Microsoft 365 Copilot is approved for use on school-managed devices. Microsoft 365 Copilot offers enterprise-grade security and compliance under the Futures Trust Microsoft 365 tenancy agreement. Access to other AI platforms may be blocked by the school web filter.

When using any AI tools, users should be aware of the limitations of the technology. In particular AI responses should be evaluated critically and not taken at face-value. The technology is rapidly changing and is subject to many limitations and may not be comprehensive or accurate.

Therefore AI-generated content should be evaluated critically and not accepted at face value. Users should avoid over-reliance on AI, in particular do not solely depend on AI for tasks that require deep understanding or creative thought. Users must avoid using AI tools to generate false, or misleading content, including images or videos, that may cause harm or distress to others, or spread disinformation or conspiracy theories.

Users should recognise that AI tools may often be used by others on-line to produce false or misleading content, including 'deep-fakes' that may cause harm, distress or offence. Through e-safety education, the school will work to educate students about the risks associated with AI and to take a responsible approach when using AI-enabled tools and services.

## **8. Personal Data**

Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (GDPR)

The GDPR is based on data protection principles that the school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

## **9. Roles and Responsibilities**

The following section outlines the broad e-safety roles and responsibilities of individuals and groups within the school.

### **The School Governors**

The School Governors are responsible for the overall effectiveness of the policy. This will be carried out by the Local Governing Body receiving regular information about e-safety incidents and monitoring reports. A member of the Local Governing Body has the role of Safeguarding Link, which includes e-safety.

### **The Headteacher and Senior Leadership Team**

The Headteacher has a duty of care for ensuring the safety of members of the school community and therefore has overall responsibility for e-safety in the school.

### **E-safety Co-Ordinator**

The Headteacher delegates much of the day to day responsibility for e-safety to an E-Safety co-ordinator who is the Designated Safeguarding Lead (DSL). The E-Safety Co-ordinator has a leading role in establishing, reviewing and implementing the school e-safety procedures, providing training and advice for staff and liaising with outside bodies in relation to e-safety issues.

### **Students**

Students should be aware of the significant risks of exposing themselves or others to personal harm or danger because of inappropriate use of IT and digital media and should manage their use of IT to minimise these risks.

Students are responsible for using the school IT systems in accordance with their AUP, and generally understanding the importance of adopting good e-safety practice when using digital technologies in and out of school.

### **Parents and carers**

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way.

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national and local e-safety campaigns and literature.

### **Staff**

Staff are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices and have read, understood and signed the staff Acceptable Use Policy (AUP). Staff that work directly with students are also responsible for helping them understand the importance of e-safety and how they can reduce exposing themselves to risk.

### **IT Services**

IT Services (specifically the network manager) is responsible for ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack and has all the necessary controls in place, such as web filtering and password protection to reduce the risk of e-safety issues arising.

## Appendix

### ICT Acceptable Use Policy for Students

#### Introduction

Technology and the internet are powerful tools, which are integral to life in and out of school. They can be used in very positive ways to enhance learning or for negative purposes such as cyber-bullying or promoting division and extreme viewpoints. PRIDE values of “Pride, Respect, Individual, Determined, Excellent” apply just as much to online behaviours.

**This Acceptable Use Policy is intended to ensure, that at all times:**

- Young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

#### Acceptable Use Policy Agreement

I understand that I must act in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the school ICT systems and other users.

#### For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of “stranger danger”, when I am communicating on-line.
- I understand that there may be times when someone tries to gain my trust on-line in order to persuade me it is safe to give them access to personal information, images/video, social media accounts or data. I will report any attempts to a trusted adult.

- I understand that not all information that I see on-line is true or accurate. I understand that the Internet is often used to spread mis-information, fake news, false images and other content that may be harmful or offensive in nature. I will report anything that I am concerned about to a trusted adult.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )
- I will not arrange to meet people off-line that I have communicated with on-line without parental knowledge and accompanied by an adult.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I will only use Artificial Intelligence (AI) tools provided by the school and I will not use these to generate false or harmful content, including images or videos. I will not use AI in any way that would cause offense, distress or harm to another person

**I understand that everyone has equal rights to use technology as a resource and:**

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for chat rooms, social media, pornography, violent or extreme content, on-line gambling, internet shopping or file sharing.
- I will not use the school systems for on-line gaming or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

**I will act as I expect others to act toward me:**

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will not take or distribute images of anyone without their permission.

**I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**

- I will not use any personal devices, including USB devices, in school without first asking permission and understand any mobile phone seen on school site is liable to be confiscated, until collected by a parent.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will **NOT** use social media on school site, or at all using school equipment.
- Where work is protected by copyright, I will not try to download copies (including music and videos)

**I understand that I am responsible for my actions, both in and out of school:**

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network /

internet, detentions, exclusions, contact with parents and in the event of illegal activities involvement of the police.

### **User's Acceptance**

By clicking "Accept" I acknowledge that I have read and understood the acceptable use policy and agree to abide by the requirements laid down.

### **Staff Acceptable Use Policy**

This is available as a separate but related policy.

## **Online Safety during Remote Learning**

The school recognises that children both on-site and off-site are vulnerable to abuse and radicalisation online. Children who are at home may be spending more time online and this increases their vulnerability.

The Hinckley School recognises that additional safeguarding arrangements are required to ensure that children are safe online at this time.

Governors will review arrangements to ensure that they continue to be appropriate. Online activity in school will continued to be monitored through our usual IT monitoring systems. This will be monitored daily by a designated member of the ICT Team who will inform the DSL and the Colleges teams so further action can be taken as necessary following the guidance in the Safeguarding and Acceptable Use Policies (Both Staff and Student).

### **Children who are not attending school**

All students have been reminded of the acceptable use policy for students which is applicable to both accessing the school's resources with The Hinckley School and externally e.g. from home. Further advice has been given to all parents/carers from the school via email and on the school website about keeping their children safe online and how to access further advice from sources such as [www.Internetmatters.org](http://www.Internetmatters.org). Students and parents have also been given information on how to report concerns externally via organisations such as CEOPS and through the school for extra support if necessary.

The school may use technology to deliver learning to pupils who are at home. In order to ensure that children are safe when learning online, the school has:

- Ensured that staff are trained are aware and understand how to use IT appropriately and where to access support when they need it.
- Provided pupils with information sheets and guidance on how to access the Teams and other resources safely.
- Pupils through their home working tasks are given guidance on which websites to access for extra research. The contents of the Acceptable use Policy agreement and accessing support safely.
- Parents have been advised on suitable websites for children, parental control settings, supervision and monitoring, where to get extra support, the contents of the acceptable use agreement of using IT for school based learning activities and the risks of using online unknown tutors etc once you have done this.
- School-issued laptops are protected with the same anti-malware software, safeguarding software, and SmoothWall Cloud Filter which provide the same protection, monitoring and filtering as any school-based computer, regardless of the Internet connection used to connect the device at home

## **Children and online safety away from school and college**

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police.

Online teaching should follow the same principles as set out in the MAT code of conduct.

The Hinckley School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

When delivering "Live Lessons", staff and students are expected to follow the guidelines below:

- No 1:1s, groups only unless specifically authorised by a member of the School Leadership Team.
- Staff and students don't have to wear uniform, but must be appropriately dressed for the lesson, in clothing suitable for being seen in public.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred.

- The live class should be recorded so that if any issues were to arise, the video can be reviewed.
- Students must sign into Teams at the beginning of the lesson using their usual school username. Any unrecognised names, 'nick-names' or guest accounts will not be admitted to the lesson
- Students can choose not to turn "video" on if you feel more comfortable with audio only.
- No other person or family member is allowed to appear or take part in the lesson
- Students must mute microphones and must not un-mute unless invited to do so by the teacher. Students must use the 'raise hand' function if they wish to ask a question
- Students must observe the same standards of conduct and behaviour as classroom-based lessons. Phones must be switched off. Teachers will remove any student from the online lesson who does not follow the behaviour expectations
- Students must not attempt to record the lesson or take photographs or screen-shots of the lesson content, the teacher, or any other student
- Students should report any concerns that arise during the lesson directly to their head of year.
- Staff should be wearing their ID badge and where possible there must be at least 2 School employees present in the video call.
- Staff must only use platforms provided by the Futures Trust MAT to communicate with pupils
- Staff should record, the length, time, date and attendance of any sessions held

### **Support for schools implementing remote learning**

- <https://swgfl.org.uk/resources/safe-remote-learning/>