Name of Policy	**E-Safety Policy**
Named Person(s)	**Gavin Burt**
Review Committee	**Governing Body**
Last review date	Autumn Term 2023
Next review date	Autumn Term 2026

Contents:

Statement of intent

This policy is intended to ensure students and staff at Highfield Middle School are protected while using digital technologies at the school.

The School is committed to including digital technologies, in particular internet use, in our curriculum. In doing so, we recognise the inherent risks posed by this useful learning tool. Full compliance with this policy will mitigate these risks and help to ensure students are safe online.

1: Introduction

1.1. While digital technology and the internet provide an exciting opportunity for students to learn and interact with various subjects, they also pose a risk, with the potential for exposure to inappropriate content and inappropriate contact from other children and adults. Digital technology also provides an opportunity for students to engage in unacceptable behaviour, both online and offline.

1.2. In order to keep students safe online, and for them to learn how to keep themselves safe online, all students and teachers should be aware of relevant skills and strategies needed to ensure internet safety.

1.3. Mitigating the risk to students created by digital technology and the internet will be ensured through specific safety lessons, assemblies and will also be embedded within the general curriculum.

1.4. E-safety will depend on policies being properly implemented at all levels of the school community: from published policies, to a secure school network design, the effective management of school broadband and filtering systems, parental awareness of the dangers of online use and effective teaching about digital-technology use.

1.5. Our school has appointed an e-safety officer to take responsibility for e-safety implementation, including updating and adoption of this policy.

1.6. This policy is to work in conjunction with our Child Protection and Safeguarding Policy, Anti - Bullying Policy, Social Media Policy, GDPR Policy, ICT Control and Security Policy and ICT Disaster Recovery Policy.

2: Aims

2.1. We are committed to using the internet and other digital technologies to:

- Make learning more engaging and effective.
- Enable students to gain access to a wide variety of knowledge in a safe way.
- Raise educational standards.
- Prepare our students for using the internet and online tools safely outside of school and throughout their education.

3: Coverage

3.1. Digital safety encompasses a number of technologies such as computers, tablet computers, Chromebooks, collaboration tools, internet technologies, mobile devices and student devices.

3.2 This policy covers all staff, students and visitors to our school.

4: E-safety Measures

4.1. The School's internet system, and access to it, is specifically designed for staff and pupil use and, as such, includes filtering appropriate for our students and staff.

4.2 All students agree to an ICT Acceptable Use Policy. This policy is reviewed regularly to ensure that they agree to and understand the policy. A copy of this policy is printed in the Student Planner for parents/carers and students to refer to.

4.2. Students will have clear objectives about why they are using the internet whenever the internet is incorporated into lessons.

4.3. Lessons using the internet will be carefully planned, taking into account student age and curriculum requirements.

4.6. Students will be taught what internet use is acceptable and unacceptable, and teachers should be vigilant during internet based lessons.

4.7. E-safety training is part of all staff induction and staff will receive regular training on e-safety to ensure all staff are well informed.

4.7. Particular vigilance is necessary if and when students are undertaking internet searching. Teachers should use their professional judgement regarding whether this internet function is appropriate for the relevant class.

4.8. Google 'safe search' is enforced automatically by our systems. Teachers should be vigilant if students use alternative search facilities and make judgement calls on their use, due to the range of content and possibility for accessing inappropriate material.

4.9. Records will be maintained detailing all staff and students internet access.

4.10 Staff must report any concerns to the E-Safety Officer both verbally and in writing on the school's safeguarding reporting system, Bromcom.

5: School policies

5.1 **Information system security**:

5.1.1 The School currently uses Schools Broadband Internet services with their appropriate firewall and all appropriate filters, along with our own procured filtering system, which is updated regularly.

5.1.2 The security of the information systems and ICT system capacity will be reviewed regularly.

5.1.3 The virus protection will be regularly updated. There are procedures in place for virus protection to be updated on any laptops used by staff members or students. An increasing reliance on Google Chromebooks is reducing the risk of viruses impacting on the systems.

5.2 **Email and digital communications**:

5.2.1 Only approved school email accounts may be used at school/via the school network. Additionally, students must not receive or access personal email accounts. All communication between staff and students should be conducted using the school email system or through Google Classroom. Additionally, staff are encouraged to only communicate with each other before 6pm, utilising the scheduled send function to promote a healthy work - life balance

5.2.2 Students should notify a teacher immediately if they receive an offensive e-mail or communication via any other means.

5.2.3 Students should be taught about the dangers involved in e-mail communications. They should be taught:

- Not to reveal personal details about themselves or others in e-mail or digital communication. This will generally include full names, addresses, mobile or landline phone numbers, school name, e-mail address, names of friends, specific interests and clubs etc.
- Never to arrange to meet someone they have 'met' via email/online without appropriate safeguarding measures (e.g. the presence of a parent or responsible adult).
- That online communications are 'real' and as such require the same respect for others as face-to-face interactions.

5.2.4 Parents and students alike should both be informed of the risks inherent in using social media. Social media websites will not be accessible to

students through the school's network and should not be accessed on school devices, unless directed by the teacher for a specific educational reason.

5.2.5 Students at our school cannot send emails to organisations or persons outside of the school, unless a specific domain has been authorised by the E-Safety officer.

5.3 **The school website**:

5.3.1 The Headteacher has overall responsibility for the content of the school website. This includes ensuring all content is appropriate and accurate. All content for the website should be checked by the appropriate people, decided by the Headteacher of the school.

5.3.2 No personal information or contact details will be published on the school's website. This extends to the use of pupil's full names. The school address, e-mail and main telephone number should be the only contact information available to website visitors.

5.3.3 The uploading of any images or photographs of students onto the school website requires parental and /or student permission. We ask this permission at the start of the year and should not post any images of students who have declined. Any images should be carefully chosen with safeguarding in mind and it is advisable that students are not easily identifiable in images. Pupil's names should never be used in conjunction with their photograph on the website. Records of which students we aren't allowed to use are maintained by admin staff and used by teaching staff before submitting photos & articles for publication.

5.4 **Managing filtering**:

5.4.1 IT Assist will work to ensure filtering systems are appropriate, efficient and as effective as possible. This will entail regular proactive checks and monitoring to evaluate the nature of the blocked sites that students are attempting to access. This will ensure that we can respond to any concerns or issues arising. Regular meetings should be held between the ICT department and the E Safety officer.

5.4.2 If staff or students discover unsuitable sites, the URL, time and date must be reported to the class teacher in the first instance and then to the ICT technicians, who should inform the E-Safety officer. There are processes in place to deal with such reports.

5.5 **Protecting personal data**:

5.5.1 Personal data will be recorded, processed, transferred and made available according to the GDPR Policy. The School follows a personalised GDPR Policy - see appendix E.

5.5.2 Personal data should be protected via encryption or password as outlined in the GDPR policy.

5.5.3 Information sharing, confidentiality, storage and protecting data is managed through the GDPR policy and staff should be made aware of this.

5.6 **Personal devices**:

5.6.1 Personal devices should be used responsibly and within the guidelines outlined in the staff code of conduct and this policy.

5.6.2 If School supplied personal devices are to be used outside of school, they should be kept secure at all times. They should always be logged out so that no user can access school information.

5.6.3 School devices are filtered and monitored when in school and accessing the school network, however staff, students and parents need to take responsibility for devices used outside of the school network and the school cannot be held responsible for usage outside of the school network.

5.6.4 School devices should only be used by school staff and not family members.

5.6.5 Personal devices should utilise a secure log on and should only be used by the person currently logged on. Users should log out or secure the device whenever they have finished using it.

5.6.6 Personal devices should have settings configured to ensure that email and other systems are secure, e.g. passwords to access each time, auto time out, auto screen lock, etc.

5.6.7 Whilst the schools try to manage access to personal devices, the school cannot be held responsible for students accessing the internet using their own data connection on their own devices.

5.7 **Complaints**:

5.7.1 Complaints regarding student misuse of the school's internet/digital devices will be dealt with by the class teacher in the first instance. More serious issues should be dealt with by the E-Safety officer. Sanctions for misuse should follow the normal behaviour policy, but may include:

- Revocation of internet use privileges
- Communication with the pupil's parents/carers
- Detention or other usual discipline methods

5.7.2 Staff misuse of the internet or digital technology should be referred to the Headteacher.

5.7.3 Any issues or complaints of a child protection nature should be dealt with according to the school's Child Protection and Safeguarding Policy procedure.

5.7.4 Information on the complaints procedure should be published on the school's website and parents should be informed about this.

5.8 **Digital technology/internet use outside of school**:

5.8.1 Parents should be informed of the inherent risks of internet use.

5.8.2 The school will be aware of, and responsive to, any issues students experience via their use of the internet or digital technology outside of school. The school's Bullying Policy may also be relevant in such instances. Issues may be referred to the police by the school, or the school may advise parents/carers to contact the police themselves in certain circumstances.

5.9 **Parents**:

5.9.1 Parents will be provided with a range of resources to support them with understanding risks online and how to get help.

5.9.2 Resources will be available via our website and will provide links to report concerns directly to CEOP (to report people involved in child sexual exploitation) and/or IWF (Internet Watch Foundation, if it is important the content needs to be removed from the Internet).

5.9.3 The information and resources will be signposted to parents at key events and via communications through the year.

6: Planned Student Curriculum

6.1 In addition to staff using opportunities to discuss and explore e-safety issues within all subject areas, there are planned opportunities built into the school year.

6.2 Where a particular incident or concern requires an immediate response, the school will implement strategies to address concerns and to educate students quickly. A response could include some of the following:

- assemblies to raise and address the issue
- letters to parents outlining the concern and strategies to address this (an example letter is in appendix C)
- external organisations involvement, e.g. police
- particular changes to our filters or security systems

6.3 In all years there are discrete planned lessons, delivered within Citizenship and/or Computing lessons covering topics such as :

- Email scams
- Hacking
- Protecting personal data

- Health and safety risks associated with digital devices and how to contain them; responsible use of digital devices
- Security risks to data and how to contain them
- The use of usernames, passwords and other security measures when accessing online systems
- Threats to and methods of preventing misuse of personal information
- Online shopping and Consumer protection
- Responsible use and acceptable behaviour
- Privacy issues associated with the use of ICT
- Safe and responsible practice when using ICT
- School and social media
- Cyber bullying and abuse
- Body image and the media
- Harassment and stalking
- Viewing harmful content
- Sharing images and the law
- Sexting
- Risks of life online
- Sharing material online
- Mental wellbeing

6.7 Assemblies regularly cover e-safety topics including sharing nudes, sharing inappropriate media, anti-bullying via social media, posting personal information, grooming, etc. These assemblies respond to different issues each year depending on the needs of our cohort.

7: Staff Training

7.1 The School is committed to ensure that all staff have the appropriate information and skills to manage, support, address and be aware of e-safety issues.

7.2 All staff, teaching staff, associate staff and trainee teachers, will have e-safety training.

7.3 Issues arising - If a key issue arises that requires immediate training and response, this will be delivered as quickly as possible to staff, via morning briefing, weekly after school sessions, staff bulletin or tutor notices, whichever is the most appropriate.

8. Monitoring

8.1. The law related to internet use is changing rapidly and staff and students need to be aware of this. Relevant laws include:

- The Computer Misuse Act 1990
- The Public Order Act 1986
- The Communications Act 2003
- The Sexual Offences Act 2003
- The Malicious Communications Act 1988
- The Copyright, Design and Patents Act 1988
- The Protection of Children Act 1978
- The Obscene Publications Act 1959 and 1964
- The Protection from Harassment Act 1997

8.2. This policy is monitored and updated to account for changes in the legal landscape, such as amendments to the outlined laws. The e-Safety officers are responsible for updating this policy and ensuring the school remains in compliance with its legal obligations.

8.3. Monitoring use - As a public organisation with responsibilities for the care of young people we will exercise our right to monitor the use of our computer systems for inappropriate use.
In order to protect our students and staff from inappropriate material, we use a number of methods of monitoring use. These include remote monitoring of screen displays and recording of the internet sites accessed by users.
We will only check user records when we believe that somebody has failed to fulfil their responsibilities.

Senso

This security software is installed on all school IT equipment and all IT equipment brought into school before it is allowed to be used on site. Senso is installed automatically upon all IT equipment brought through school.
Senso provides us with full visibility of pupils' machines, with the power of key logging and live screen to capture any threats early. The Senso cloud allows us to view the pupil's screen as they are working, with the added protection of keyword, application and web blocking.
It is designed with the UK Government Prevent duty, UK Safer Internet Centre, the UK Department for Education's Keeping Children Safe in Education (KCSiE) guidance and with keyword and Illegal URL lists from the Internet Watch Foundation (IWF) in mind. Utilising specialised keyword lists, Senso is able to detect violations and capture evidence of computer and internet misuse so that we can view and decide on any necessary action if required.

9: Acceptable Use Policy

9.1 The acceptable use policy is to be shared, discussed and agreed with all students as they join the school and with all staff.

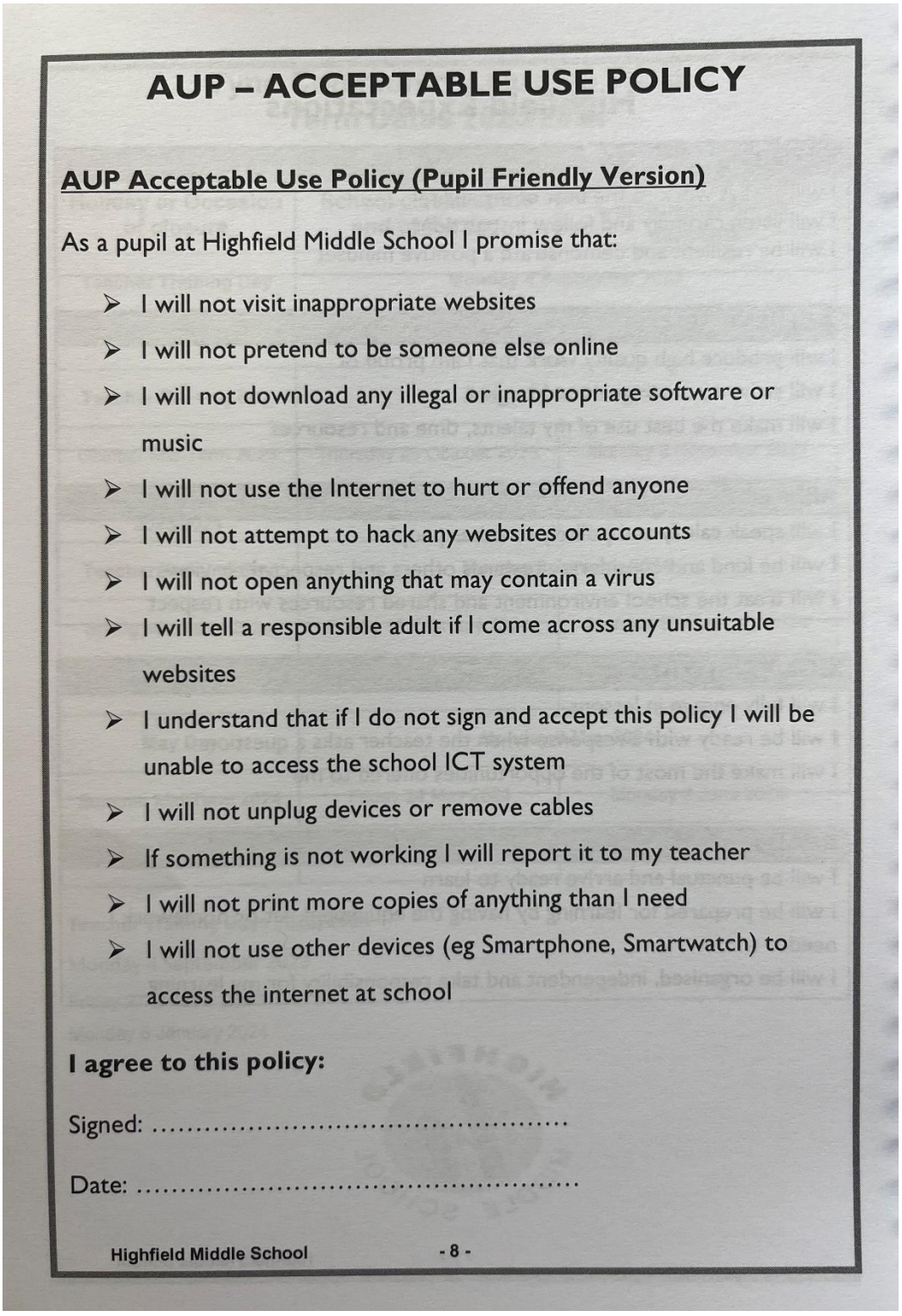
9.2 The AUP will be available to students and parents/carers via their school planner so that they can reference the content when needed. Students sign annually to agree that they will abide by the policy.

9.3 A separate AUP must be discussed, agreed and signed by all staff working in the school.

Appendix A: AUP

ACCEPTABLE USE POLICY (AUP) FOR STUDENTS

This document is included in our student planners and is signed at the start of each year.



AUP – ACCEPTABLE USE POLICY

AUP Acceptable Use Policy (Pupil Friendly Version)

As a pupil at Highfield Middle School I promise that:

- I will not visit inappropriate websites
- I will not pretend to be someone else online
- I will not download any illegal or inappropriate software or music
- I will not use the Internet to hurt or offend anyone
- I will not attempt to hack any websites or accounts
- I will not open anything that may contain a virus
- I will tell a responsible adult if I come across any unsuitable websites
- I understand that if I do not sign and accept this policy I will be unable to access the school ICT system
- I will not unplug devices or remove cables
- If something is not working I will report it to my teacher
- I will not print more copies of anything than I need
- I will not use other devices (eg Smartphone, Smartwatch) to access the internet at school

I agree to this policy:

Signed: .....

Date: .....

Highfield Middle School - 8 -

Appendix B: Staff Acceptable Use Policy

Acceptable Use Policy- Requirements of Staff:

Safeguarding

1. As a member of staff you have responsibility to protect and safeguard our students. Care must be taken when accessing any IT facilities and staff should be vigilant at all times. Staff should be proactive in checking what students are accessing and what they are doing when using any IT facilities.
2. Staff should look for opportunities to discuss e-safety with students to promote positive and safe usage.

Devices/Login

3. You are responsible for your individual account and must take all reasonable precautions to prevent others from being able to use it. You must not disclose any passwords or login details to anyone other than the persons responsible for running and maintaining the school's ICT systems.
4. You must not use a computer that has been logged in under another student's or teacher's name.
5. You must not log in using another person's login and password.
6. If you use a personal device such as a tablet, laptop, smart phone, you are wholly responsible for that device and its use. You must ensure that the device is safe and secure and that no other user uses the device whilst logged on with your username. You must ensure that you have logged out of any device when you have finished using it.
7. You must secure any device if you are moving away from it even for a short space of time. You could do this on a Windows PC by pressing CTRL, ALT and DELETE to lock the PC. Chromebooks - simply closing the lid should lock it. Mobile phones and tablets should be secured with a PIN.
8. Mobile phones, tablets and smart watches are not to be used for personal use around students. Bluetooth must be turned off and the device must only be used for appropriate educational purposes.

Personal Information

9. You must not post personal contact information about yourself, including your address, telephone number, school address etc. This information must not be provided to an individual, organisation or company, including websites that solicit personal information.
10. The use by students of names, photographs or recordings of staff, or any member of the school community is not permitted. Any exception to this rule must receive prior approval from the Headteacher.

Downloading/Uploading

11. Downloading software, or other program files, is forbidden without prior consent from persons responsible for running and maintaining the school's ICT systems, as is the use of illegal / pirated content.

Unsuitable Material/Cyber Bullying/Social Networks

12. Under no circumstances should you view, upload, download or post any material that is likely to be unsuitable. This applies to any material of a violent, dangerous or inappropriate nature, sexual content and includes the use of abusive language. Any material designed to incite hatred or that has the purpose or effect of violating a person's dignity or creates a degrading, humiliating, hostile, intimidating or offensive environment should also not be accessed.
13. Use of non-school social networking sites such as Facebook, Tik Tok, Instagram, Snapchat and Twitter etc. are not permitted within school, this extends to access via personal, mobile related devices, during the school day.
14. Access to school related social media sites should only be done once you have approved access agreed via the Social Media Policy.
15. You must respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner. If you have questions about copyright, ask the School's IT team.
16. You should check the suitability of the contents of any sites or materials that you are directing students to prior to the lesson.

User Areas

17. All electronic files created or stored using the school's IT systems, remain the property of the School. The School will try to protect the privacy of staff, however when a breach of the AUP is suspected, then email and file storage may be checked by IT staff under the supervision of a Head or Deputy Headteacher.
18. You should not keep personal documents on the school system.
19. Files should only be kept for as long as required and be in line with the GDPR policy.

Email/Messaging

20. Students and staff are responsible for email, chat, blog or any other messages they send / submit and for contacts made. Messages should be written carefully and politely. Users should not assume that such messages will always be private.
21. Staff should only use School provided systems for School work and not for personal use.

22. Confidential or inappropriate information must not be sent via email or any other method. However Google to Google email is currently encrypted and is suitable for sending confidential information, subject to adherence to the GDPR policy.
23. Email with attachment(s) from an unknown source should be deleted.
24. Unsolicited, or anonymous, email (including chain emails, virus warnings and phishes) should be reported immediately to a person responsible for running and maintaining the school's ICT systems. Under no circumstances should these be forwarded on to other staff or students.
25. As a user of the school ICT facilities, you have a responsibility to promptly disclose to IT technical staff any message you receive that is inappropriate or makes you feel uncomfortable.

In conclusion, under the terms of Highfield Middle School AUP, no activity may be undertaken that could be in any way construed as bringing the School's name into disrepute.

Signed: _____

Role: _____

Date: _____