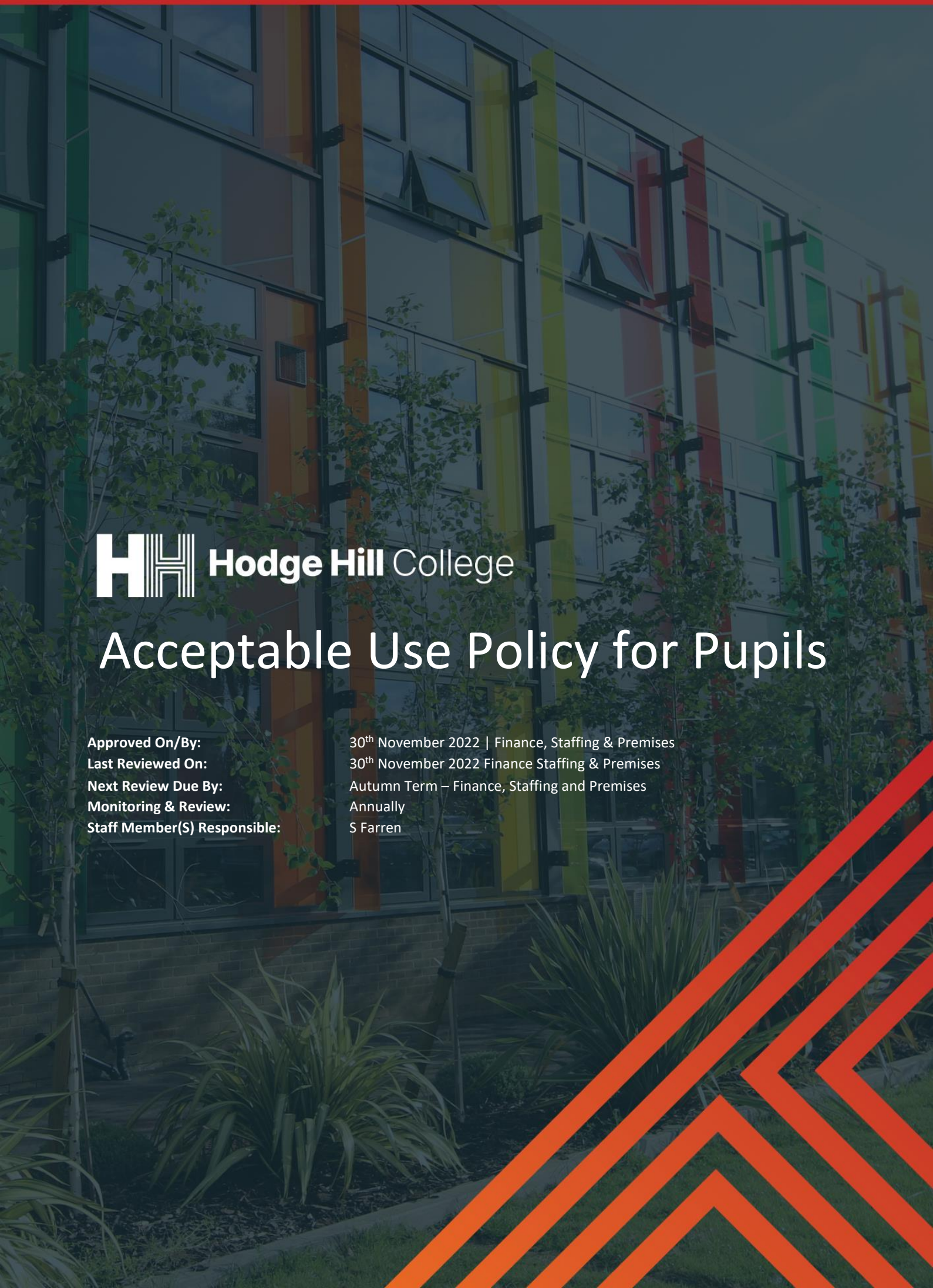

Hodge Hill College

Acceptable Use Policy for Pupils

Approved On/By:	30th November 2022 | Finance, Staffing & Premises
Last Reviewed On:	30th November 2022 Finance Staffing & Premises
Next Review Due By:	Autumn Term – Finance, Staffing and Premises
Monitoring & Review:	Annually
Staff Member(S) Responsible:	S Farren

1. Introduction

1.1 Hodge Hill College recognises the essential and important contribution that technology plays in promoting children's learning and development, both at school and at home. All pupils within our College have the opportunity to use a range of IT resources, including internet access, as an essential part of learning. This includes access to:

- Computers, laptops and other digital devices
- Internet Services to access learning platforms
- Digital cameras

1.2. This policy sets out the expectations of the school for pupils in how they use and interact with IT systems in schools. It will be reviewed annually.

1.3. This policy links to other policies, including:

Behaviour Policy
Safeguarding Policy
Data Protection Policies
Family Handbook
Sex and Relationships Education (SRE) Policy

Pupils will be notified of this policy via the Impero logon screen, which will appear each time they logon.

2. Aims

2.1. Hodge Hill College seeks to ensure that all Pupils are safe and responsible users of technology. We will support our pupils to:

- Use our resources and technology safely, carefully and responsibly, respecting system security and password security policies
- Be kind online and help us to create a community that is respectful and caring, on and offline
- Be safe and sensible online, and always know that all pupils can talk to a trusted adult if they are unsure or need help.

2.2. **We value the importance of safe behaviour**. Deliberately uploading or adding any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community, misuse or deliberate damage to school equipment, using technology without permission and at times that are not allowed, or bypassing school filtering and monitoring systems (this includes, but is not limited to, the use of VPN, personal hotspot devices, attempting to change school computer settings, using portable apps and anonymous browsers) will be dealt with according to our schools' Behaviour and Anti-Bullying policies.

2.3. **We recognise there are potential risks**. Hodge Hill College will take all reasonable precautions including monitoring and filtering systems, to ensure that pupils and staff are as safe as possible when using school equipment, our internet and systems. This monitoring will be proportionate and will take place in accordance with data protection (including GDPR), privacy and human rights legislation. Hodge Hill College reserves the right to monitor the activity of all users on school systems. We will refer to Saferinternet.org.uk provider self-certification when selecting providers to ensure they meet appropriate safety standards.

2.4. We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace and will regularly review the methods used to identify, assess and minimise online risks, as well as examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted. Hodge Hill College cannot be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

2.5. Hodge Hill College owned information systems, including Wi-Fi, must be used lawfully. The Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

2.6. We recognise that no technical system can replace online safety education. Our staff will:

- Embed online safety education in curriculum delivery, wherever possible.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Have an awareness of e-safety issues through regular training
- Take appropriate action where necessary

2.7. Some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss. We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils and seek input from specialist staff as appropriate, including the SENCO and Child in Care Lead.

2.8. We believe that pupils and parents have an important role to play in developing responsible behaviour. To support our schools in developing pupils' knowledge and understanding about online safety, we will share this policy with pupils in school and encourage parents to read and discuss the policy with the children at home.

2.9. We ask all parents to support our approach to online safety by role modelling safe and positive online behaviour, such as sharing images, text and video responsibly, and by discussing online safety whenever children access technology at home. Parents and pupils should check the age of consent

2.10. Students or parents can speak with the Designated Safeguarding Lead at school about any concerns.

2.11. We encourage pupils and parents to find out more information via other websites such as:

www.childnet.com	www.internetmatters.org
www.nspcc.org.uk/onlinesafety	www.thinkuknow.co.uk
www.saferinternet.org.uk	

3. Pupil Agreement

3.1. Pupils are permitted to use IT systems on the following conditions:

1. I will only use ICT systems in school, including the internet, learning platforms, mobile technologies, etc. for school purposes only.
2. I will not download or install software on school technologies.
3. I will only log on to the school network/learning platforms with my own user name and password.
4. I will follow the schools ICT policies and not reveal my passwords to anyone and change them regularly.
5. I will not tamper with any connected device and not insert any USB pen into the Computer.
6. I will not damage or deface any school IT system or equipment.
7. I will make sure that all ICT communications with pupils, teachers or others are appropriate and only using authorised systems.
8. I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
9. I will report any concerns with others or mine online safety to a member of staff immediately.
10. I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
11. I will not access any chat/forum services whilst on the school network.
12. I will ensure that my online activity inclusive of social networking sites, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring them into disrepute.
13. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
14. I will respect the privacy and ownership of others' work at all times.
15. I will not attempt to bypass the internet filtering system and this includes installing any proxy or VPN connection.
16. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available on request to teachers.
17. I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer will be contacted.