

## 1. SAFEGUARDING - ONLINE SAFETY POLICY

### If you are worried about a child:

1. If it is an emergency phone 999
2. Inform the DSL Liz Bedford [ebedford@shsk.org.uk](mailto:ebedford@shsk.org.uk) or any one of the DDSLs, Helen Nash, Kay Taylor, Nina Bass and Rachel Green (contact details in table below)
3. Alternatively, if you have significant concerns you can contact the MASH directly  
0345 050 7666

### If you have concerns about an adult's behaviour in or linked to school:

1. Inform the Head Sarah Rollings [head@shsk.org.uk](mailto:head@shsk.org.uk) / 01235 546173
2. Or if your concerns are about the Head, the Chair of Governors Sara Benbow  
[S8benbow@shsk.org.uk](mailto:S8benbow@shsk.org.uk)
3. Alternatively, you can contact the LADO (see below)

### Key contact details for safeguarding in the local area

|                                                |                                                                                                                                                                |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local Authority Designated Officer             | Jo Lloyd<br><br>TEL: 01865 810603<br><br>EMAIL: <a href="mailto:lado.safeguardingchildren@oxfordshire.gov.uk">lado.safeguardingchildren@oxfordshire.gov.uk</a> |
| Locality and Community Support Service (South) | TEL: 0345 2412608<br><br>EMAIL: <a href="mailto:LCSS.South@oxfordshire.gov.uk">LCSS.South@oxfordshire.gov.uk</a>                                               |
| Multi-Agency Safeguarding Hub – Oxfordshire    | TEL: 0345 050 7666 / 0333 014 3325<br><br>OUT OF HOURS: 0800 833408                                                                                            |
| Multi-Agency Safeguarding Hub - Berkshire      | TEL: 01635 503090<br><br>EMERGENCY OUT OF HOURS: 01344786543                                                                                                   |
| NSPCC Whistleblowing Advice Line               | ADDRESS: Weston House<br>42 Curtain Road<br>London<br>EC2A 3NH<br><br>TEL: 0800 028 0285                                                                       |

|                                                    |                                                                                      |
|----------------------------------------------------|--------------------------------------------------------------------------------------|
|                                                    | EMAIL: <a href="mailto:help@nspcc.org.uk">help@nspcc.org.uk</a>                      |
| <b>NSPCC Report Abuse in Education Advice Line</b> | TEL: 0800 136 663<br>EMAIL: <a href="mailto:help@nspcc.org.uk">help@nspcc.org.uk</a> |

### **Key External Contact Details**

|                                                                     |                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Disclosure and Barring Service</b>                               | ADDRESS: DBS customer services<br>PO Box 3961<br>Royal Wootton Bassett<br>SN4 4HF<br><br>TEL: 03000 200 190<br><br>EMAIL: <a href="mailto:customerservices@dbb.gov.uk">customerservices@dbb.gov.uk</a>                                               |
| <b>Teaching Regulation Agency</b>                                   | ADDRESS: Teacher Misconduct<br>Ground Floor South<br>Cheylesmore House<br>5 Quinton Road<br>Coventry<br>CV1 2WT<br><br>TEL: 0207 593 5393<br><br>EMAIL: <a href="mailto:misconduct.teacher@education.gov.uk">misconduct.teacher@education.gov.uk</a> |
| <b>OFSTED Safeguarding Children</b>                                 | TEL: 0300 123 4666 (Monday to Friday from 8am to 5pm)<br><br>EMAIL: <a href="mailto:CIE@ofsted.gov.uk">CIE@ofsted.gov.uk</a>                                                                                                                         |
| <b>UK Safer Internet Centre professional online safety helpline</b> | TEL: 0344 381 4772<br><br>EMAIL: <a href="mailto:helpline@saferinternet.org.uk">helpline@saferinternet.org.uk</a>                                                                                                                                    |
| <b>Independent Schools Inspectorate</b>                             | TEL: 0207 6000100<br><br>EMAIL: <a href="mailto:concerns@isi.net">concerns@isi.net</a>                                                                                                                                                               |

### **Key School Contact Details**

|                  |                                              |
|------------------|----------------------------------------------|
| <b>Governors</b> | <b>Chair of Governors</b><br><br>Sara Benbow |
|------------------|----------------------------------------------|

|                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                | EMAIL: <a href="mailto:S8benbow@shsk.org.uk">S8benbow@shsk.org.uk</a><br><br><b>Nominated Safeguarding Governor</b><br><br>Bernadette Stubley<br><br>EMAIL: <a href="mailto:bstubley@shsk.org.uk">bstubley@shsk.org.uk</a>                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Designated Safeguarding Lead (“DSL”) {and Deputy Designated Safeguarding Lead (“DDSL”)}</b> | <b>Main DSL for the School</b><br>Liz Bedford<br>EMAIL: <a href="mailto:ebedford@shsk.org.uk">ebedford@shsk.org.uk</a><br><b>Deputy DSLs</b><br>Nina Bass (Junior)<br>EMAIL: <a href="mailto:nbass@shsk.org.uk">nbass@shsk.org.uk</a><br>Rachel Green (Junior)<br>EMAIL: <a href="mailto:rgreen@shsk.org.uk">rgreen@shsk.org.uk</a><br>Kay Taylor (Lower)<br>EMAIL: <a href="mailto:ktaylor@shsk.org.uk">ktaylor@shsk.org.uk</a><br>Helen Nash (Middle)<br>EMAIL: <a href="mailto:hnash@shsk.org.uk">hnash@shsk.org.uk</a><br>Sophia Scott-Malden (Sixth Form)<br>EMAIL: <a href="mailto:sscott-malden@shsk.org.uk">sscott-malden@shsk.org.uk</a> |
| <b>Designated Teacher for Looked After Children</b>                                            | Liz Bedford<br>EMAIL: <a href="mailto:ebedford@shsk.org.uk">ebedford@shsk.org.uk</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Head</b>                                                                                    | Sarah Rollings<br>TEL: 01235 546173<br>EMAIL: <a href="mailto:head@shsk.org.uk">head@shsk.org.uk</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## ASSOCIATED POLICIES

There are three policies that comprise the Safeguarding Group: Child Protection, Prevent, and Online Safety. This policy focuses on safeguarding in terms of online safety.

The Safeguarding Policy Group has alongside it a range of other important policies that work together to safeguard the individuals at this school. These policies are: Whistleblowing, Anti-bullying, ICT Acceptable use, Equal Opportunities, Safer Recruitment, Relationships and Sex Education, Health and Safety, Pastoral Care, Behaviour, Work Experience, Staff Code of Conduct and Data Protection (including the data protection impact assessment)

In writing the Safeguarding policies we have referred to: Keeping Children Safe in Education (September 2025) (KCSIE); Meeting digital and technology standards in schools and colleges (2023), Teaching online safety in schools (2023) Disqualification under the Childcare Act 2006 (September 2018) What to do if you're worried a child is being abused (March 2015) Working Together to Safeguard Children (2026); Prevent Duty Guidance: for England and Wales (2023). The use of social media for on-line radicalisation (July 2015) Harmful online challenges and online hoaxes (2021), UKCIS external visitors guidance (2022) Teaching online safety in schools (2023)

## AIMS

St Helen and St Katharine places safeguarding at the heart of all that we do; we recognise the wide-ranging aspects of the term.

The aim of this policy is to:

1. Make clear the arrangements in place in the school to protect children from potentially harmful and inappropriate online material. This includes the mechanisms to identify, intervene and escalate concerns, where appropriate.
2. Outline the systems, processes and training to safeguard, protect and educate students and staff.
3. Ensure that all members of the school community are aware of online/digital behavioural expectations. Unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
4. Set out the key principles expected of all members of the school community with respect to the use of digital technologies.
5. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community.

## SCOPE

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

**Content:** being exposed to illegal, inappropriate or harmful content, for example pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

**Contact:** being subjected to harmful online interaction with other users; for example; child to child pressure, hoaxes and challenges, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

**Conduct:** personal online behaviour that increases the likelihood of, or causes harm; for example, making sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, (including the use of generative AI) sharing other explicit images and online bullying.

**Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.<sup>1</sup>

## Summary of actions

| Element  | Key actions                                                                      |
|----------|----------------------------------------------------------------------------------|
| content  | Filtering-Smoothwall Staff and Student AUP <sup>2</sup>                          |
| contact  | Smoothwall, Personal Development (PD) lessons, Computing curriculum              |
| conduct  | Smoothwall, PD, AUP                                                              |
| commerce | Smoothwall, teacher and student education in online safety, Computing curriculum |

## ROLES AND RESPONSIBILITIES

The Head has a duty of care for ensuring the safety (including online safety) of members of the school community; responsibility for students is delegated to the Designated Safeguarding Lead (Pastoral Deputy Head (PDH)) and the Senior Deputy Head. The Head,

---

<sup>1</sup> KCSIE (2024)

<sup>2</sup> AUP Acceptable Use Policy

Designated Safeguarding Lead and Senior Deputy Head are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see below).

The managed service provider is Class Technology Solutions Ltd (CTS) responsible for ensuring that the School's IT infrastructure is secure and is not open to misuse or malicious attack; that the school meets required online safety technical requirements; and that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed. Provision will be reviewed regularly by the Director of Finance and Operations and the managed service Network Manager.

Teaching and support staff are responsible for ensuring that they have an up-to-date awareness of online safety matters and of the current School policies and practices; staff are expected to follow the school's policies on IT and Communications, Social Media and Data Protection, available in the staff area of SharePoint.

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography.

Staff must report any suspected misuse or problem to the PDH and all their digital communications with students and parents/carers and colleagues should be on a professional level.

Students are responsible for using the school's digital technology systems in accordance with the ICT Acceptable Use Policy - Students.

## **USE OF TECHNOLOGY – POLICY & PROCEDURE**

Clear guidance on the use of technology in the classroom and beyond for all users, including staff, students and visitors that references permissions/restrictions and agreed sanctions is found in the following documents, which should be read in conjunction with this policy:

- **The ICT Acceptable Use Policy – Students:** available to students, parents/carers on the parent portal. All students must have read and agreed to the full AUP. A summary of this document is displayed to students at login, and they must click their acceptance to continue. The summary version is also in their planners. A copy of both versions is in the Appendices following this policy.
- **IT and Communications Policy, Social Media Policy and Data Protection Policy:** available to staff in the Employment Policies Handbook in the Staff area of SharePoint. Staff are expected to follow these policies at all times.
- **Visitors:** Visitors do not have access to the school network. If they need access to our wifi they are given a temporary time-limited code and when they sign on, they agree to the AUP.

## **TECHNICAL PROVISION, INCLUDING FILTERING AND MONITORING**

School technical systems are managed in ways that ensure that the school meets recommended technical safety requirements and there are regular reviews and audits of the safety and security of School technical systems. Servers, wireless systems and cabling are securely located, and physical access is restricted.

All users will have clearly defined access rights to School technical systems and devices. All users are provided with a username and secure password by the managed service provider, who keeps an up-to-date record of users and their usernames. Users are responsible for the security of their username and password. Staff are required to change their secure password

at least once a year. Passwords for staff must be at least 15 characters in order to make them more secure.

The administrator passwords for the School's IT systems, used by the managed service provider, are available to the Director of Finance and Operations and kept in a secure place.

The managed service provider ensures network security through use of Sophos anti-virus software.

The managed service provider is responsible for ensuring that software licence records are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Internet access is filtered for all users on the school's network, whether accessing this from a domain joined device or using their own device (BYOD). Filtering is applied to ensure student safety alongside allowing the curriculum to be taught effectively and to that end different levels of filtering are applied to staff, Sixth Form students and students in the rest of the school.

The managed service provider maintains Smoothwall Filter - internet filtering service on both the main and back-up internet feeds. Filtering protocols for staff, students and visitors on School and own devices are agreed between Class Technology Solutions Ltd (CTS), the Senior Deputy Head and the Pastoral Deputy Head. These are reviewed continually and a self-assessment carried out using the DfE 'plan technology for your school' tool.

The managed service provider also administers the Smoothwall Monitoring system on all network-joined devices. Any reports of concerns about students are reported to the Pastoral Deputy Head and concerns about staff to the Head through the Smoothwall Monitor notification service. Smoothwall has agreed protocols for communication with School staff based on the urgency and severity of the concern, which includes but is not limited to direct telephone contact with the Pastoral Deputy Head and the Head. The Deputy Director of Operations takes on this role for external lets and is consequently DSL trained.

The school recognises that students potentially have access to 3G, 4G and 5G using their phones. Students in years 5-10 hand in their phones for the duration of the school day. Students in year 11 may only access their phones with the permission of a teacher. The sixth form can use them whenever they are in the sixth form centre or in lessons, with the agreement of a teacher. Students are frequently reminded about online safety and behaviour as accessing 3G, 4G and 5G will give them unfiltered access to the internet. The behaviour policy applies to misuse of digital technology in any context.

Smoothwall provide technical and physical monitoring for the school of all computer activity by staff and students on domain-joined devices. In the event of behaviour registering a concern Smoothwall has agreed protocols for communication with School staff based on the urgency and severity of the concern, which includes but is not limited to direct telephone contact with the Pastoral Deputy Head and the Head. The Deputy Director of Operations takes on this role for external lets and is consequently DSL trained.

## **PROFESSIONAL DEVELOPMENT**

All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and supporting policies and procedures. Online safety refresher training is delivered at least annually through staff meetings, safeguarding updates, speakers and webinars as appropriate.

## **ONLINE SAFETY IN THE CURRICULUM**

Online safety should be present as appropriate across the curriculum. Staff reinforce online safety messages through their teaching and in pastoral contact, to promote responsible and

resilient use of digital technologies by students and ensure they are well-placed to protect themselves.

A planned online safety curriculum is provided as part of the Computing, Personal Development schemes of work. This is reviewed annually by the Pastoral Deputy Head, Head of Computer Science and eLearning lead, Heads of Junior Department, and Head of PD. Online safety messages are reinforced as part of the planned programme of assemblies and pastoral activities. Students are taught to be critically aware of the materials they access on-line and be guided to validate the accuracy of information. They are also taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

## **REPORTING MECHANISMS**

Students who have breached the acceptable use policy (where no illegality is identified or suspected) should be reported to the Pastoral Deputy Head who will work with the Senior Deputy Head and managed service provider to investigate, decide on a course of action and recommend/apply sanctions where necessary. It may also be appropriate to consider reporting the issue as a safeguarding matter. In the event of the incident relating to a member of staff this will be referred to the Head and HR Manager. This may be recorded as a 'low level concern' (See Child Protection Policy) or subject to disciplinary action.

Where illegal materials or activities by students are found or suspected this should be reported to the Pastoral Deputy Head. The Pastoral Deputy Head will then inform the Head and other agencies, for example the police or children's services, as appropriate. (See Child Protection policy)

Issues regarding staff will be reported to the Head. These will be handled in compliance with School's Child Protection policy and procedures. As appropriate, issues related to staff will be reported by the Head to the LADO/police and subsequent steps will be determined by their response and in conjunction with the school's disciplinary policies and procedures. If the Head is suspected to be the perpetrator it will be reported to the Chair of Governors who will report it to the LADO/police, as appropriate.

## **SUPPORT FOR PARENTS & CARERS**

The school recognises that some parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school therefore seeks to provide information and awareness to parents and carers through the Pastoral advice area for parents on the portal. Other information may also be sent home, such as warnings passed on by local agencies e.g. ESAT<sup>3</sup>, as appropriate. Online safety is also a key element of advice given at Welcome evenings.

## **GDPR**

The school is fully committed to compliance with the requirements of the Data Protection Act 2018 (DPA 2018), which came into force on the 23rd of May 2018 and the UK General Data Protection Regulation (UK GDPR). The school will therefore follow procedures that aim to ensure that all employees who have access to any personal data held by or on behalf of the school, are fully aware of and abide by their duties and responsibilities under the DPA 2018. (See Data Protection Policy).

Staff are expected to follow the school's policies on IT and Communications, social media and Data Protection, available in the Employment Policies Handbook.

---

<sup>3</sup> Education Safeguarding Advisory Team

DPA and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. If in any doubt about sharing information, staff should speak to the Pastoral Deputy Head (DSL) or a Head of Section (DDSL). Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare of children.

### **GOVERNOR SCRUTINY**

The Chair of the Governance Committee reviews this policy to ensure that it has the relevant content. The DSL meets with this Governor at least once a term to update them on any issues. This Governor carries out regular checks of staff to ensure practice is followed. Online safety is a standing item on the Governance committee agenda, There are written termly updates to all Governors from the DSL.

|                                                                           |                                                  |
|---------------------------------------------------------------------------|--------------------------------------------------|
| <b>Policy reviewer:</b>                                                   | <b>Pastoral Deputy Head in consultation with</b> |
| <b>Senior Deputy Head and Head of Computer Science and eLearning Lead</b> |                                                  |
| <b>Policy last reviewed:</b>                                              | <b>Lent 2026</b>                                 |
| <b>Next review due:</b>                                                   | <b>Lent 2027</b>                                 |
| <b>Audience:</b>                                                          | <b>Staff/Parents</b>                             |



## **APPENDIX 1**

### **ICT Acceptable Use Policy – Students**

*The next digital literacy won't be about the nuts and bolts of how to use the web or a mobile phone, but how to set boundaries about when we let them encroach on our downtime.*

Aleks Krotoski

#### **Aims**

The school aims that students have good access to digital technologies, and, in return, expects students to agree to be responsible users.

#### **Acceptable Use Policy Agreement**

I understand that this Acceptable Use Policy is an extension to the school rules and forms a contract between me and the school.

I understand that this contract applies every time I use technology in the school, including BYOD.LE

I understand that if I use my own digital technology in the school day/on school premises/on a school trip that I will still follow these rules.

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 internet, and referral to my Head of Section, Pastoral Deputy Head, or the Head.

### **For my own safety:**

I understand that I must use school ICT systems in a responsible way, to minimise risk to me, to other users, and the school systems.

Therefore, I will:

- Keep my username and password secure.
- Log out of my computer when I finish using it.
- Be aware of the potential dangers of messaging strangers online.
- Report to a responsible adult any unpleasant or inappropriate material, or anything that makes me feel uncomfortable, when I see it online.
- Report to an adult if I feel bullied or abused online, or if I receive any offensive or inappropriate images, including nude or semi-nude pictures (sexting)

I will not:

- Share my password.
- Try to use anyone else's username and password
- Share my personal information online
  - (e.g. name, address, telephone numbers, age, gender, educational details, financial details).
- Share other people's data online.
- Meet strangers that I met online. If I decide to, I know I should do so in a public place and take an adult with me.
- Tolerate offensive behaviour from my peers and will always report it.

### **I understand that everyone has equal rights to use technology:**

- 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 try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will use printers responsibly and try to avoid wasting resources.

### **I will treat others as I would like to be treated:**

- I will be polite and responsible when I communicate with others, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions. I will recognise that what I might consider 'banter' others might find offensive or abusive.
- I will not send or make anything which is offensive, abusive, obscene or defamatory or which may be unlawful (e.g. sexting) or material which might cause embarrassment to the school.
- I will not take or share pictures or videos of the school or anyone in the school without permission.
- I will not share confidential information about staff, students, or parents.
- I will respect others' work and will not access, copy, remove, or alter other people's files, without their permission.
- I will not use other people's work without permission.

- If I use other people's work, I will reference it. I can learn how to reference in the library.
- If I use other people's work without their permission or giving them credit this is a breach of copyright, and I could get in trouble.
- I will not make any other statement which is likely to create any legal liability (whether criminal or civil, and whether for me or the school);

**The School has a responsibility to maintain the security of the technology I use. Therefore:**

- I will treat computers carefully and immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open hyperlinks or attachments to emails, unless I know and trust the person who sent the email.
- I understand that my files may be deleted if they pose a threat to the system.
- I will not install programs on any school device, nor will I try to alter computer settings.

**Artificial Intelligence (AI) or a Large Language Model (LLM) e.g. Chat GPT can be helpful in my schoolwork, but I will follow some guidelines:**

If I use AI/LLM to complete assessed or marked schoolwork, I will check with my teacher that this will be appropriate and helpful for my learning.

I will make clear what is my work and what has been created with AI/LLM help.

**When going online, I recognise that:**

Access to the internet is provided for academic research, completing schoolwork, and to communicate/collaborate with other members of the school community.

When I am using the internet to find information, I should take care to check that it is accurate information. I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me and/or to put across biased or extreme views.

In school, teachers will guide me towards appropriate materials. Outside school, my families are responsible for helping me.

All internet access is subject to filtering and content control, to minimize access to inappropriate material. All internet access in school is logged, monitored and traceable.

I will not use tools like Virtual Private Networks (VPNs) or any other software to deliberately bypass the school's filtering/security systems.

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

- I will not use the school systems or devices for gaming, gambling, shopping, social media, unless I have permission of a member of staff to do so.

- I understand that the school also has the right to take action against me if I am involved in inappropriate behaviour. I am also responsible for my behaviour outside of school and I understand that the school will never tolerate abusive behaviour by one student towards another (e.g. cyberbullying).
- I will ensure that if I am joining lessons or other events remotely, I will follow the expected standards of dress, and ensure I am working in an appropriate environment.
- I understand that I must not record film or take photos during lessons, or around school (even if this is just of myself) unless given express permission to do so by a member of staff. I must not post images or videos online that have been filmed within school.

|                                                                           |                                                  |
|---------------------------------------------------------------------------|--------------------------------------------------|
| <b>Policy reviewer:</b>                                                   | <b>Pastoral Deputy Head in consultation with</b> |
| <b>Senior Deputy Head and Head of Computer Science and eLearning Lead</b> |                                                  |
| <b>Policy last reviewed:</b>                                              | <b>Lent 2026</b>                                 |
| <b>Next review due:</b>                                                   | <b>Lent 2027</b>                                 |
| <b>Audience:</b>                                                          | <b>Staff/Student</b>                             |

## **Appendix 2-Summary version for Planner and use when accessing school systems**

### **ICT Acceptable Use Policy – Y7-U6**

- 1. Use technology safely and responsibly**  
Whether it's school devices, your own phone, or AI tools, at school, home or on a trip, use technology in a way that keeps you and others safe.
- 2. Protect your accounts**  
Keep your username and password secret. Don't use other people's accounts and always log out when you're finished.
- 3. Stay safe online**  
Don't share personal information, talk to strangers, or arrange to meet anyone you've only met online. Report anything that makes you feel uncomfortable.
- 4. Be kind and respectful**  
No cyberbullying, rude messages, offensive "banter," or sharing harmful content (including nude or semi-nude images). Treat others online the way you want to be treated.
- 5. Use school technology for learning first**  
Don't waste internet bandwidth by streaming, gaming, shopping, or using social media unless a teacher gives permission. Access to the internet is filtered and monitored to keep you safe, don't try to get around this.
- 6. Respect property and privacy**  
Don't access, change, or copy other people's files. Don't take photos or videos of anyone (or the school) without permission.
- 7. Keep devices and systems safe**  
Don't install software, change settings, use VPNs, or open suspicious links or attachments. Report any damage or faults immediately. Use printers responsibly.
- 8. Use information and AI/LLMs honestly**  
Check that information you find online is accurate. If you use AI/LMM tools, only do so with your teacher's permission and make sure you reference it properly.

9. **Avoid illegal or inappropriate content**

Never try to access or share anything harmful, offensive, extremist, pornographic, discriminatory, or copyrighted without permission.

10. **Your actions have consequences**

School can take action for misuse both in and out of school. Breaking the rules may lead to losing ICT access or further disciplinary steps.

## **ICT Acceptable Use -Junior Department**

1. **Use technology safely**  
I will use computers, iPads, and the internet in a way that keeps me and others safe.
2. **Keep my password secret**  
I won't share my password or use someone else's login.
3. **Stay safe online**  
I won't share personal information like my name, address, or school online.
4. **Tell an adult if something is wrong**  
If I see anything that upsets me or feels wrong, I will tell a teacher or trusted adult straight away.
5. **Be kind online**  
I will use friendly words and be polite. I won't send or look at unkind or rude messages.
6. **Use school devices properly**  
I'll only use the internet, apps, and games that my teacher says are okay.
7. **Look after equipment**  
I will treat computers, tablets, and other devices with care and report any problems.
8. **Don't take photos or videos without permission**  
I will only take pictures or videos if a teacher says it's allowed.
9. **Use information honestly**  
If I use ideas from the internet or AI tools, I will ask my teacher and say where I got the information.
10. **I know there are consequences**  
If I break these rules, I may lose ICT privileges and my teacher will talk to me about what happened.