LIONHEART

SCHOOL

Online Safety Policy

November 2025 – November 2027

Table of Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

- Searching, screening and confiscation

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

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

This policy complies with our funding agreement and articles of association.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches students how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs.

All governors will:

- Make sure they have read and understand this policy.

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school approach to safeguarding and related policies and/or procedures.
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks students face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The ICT Manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting a full security check and monitoring the school's ICT systems monthly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All Staff and Visitors

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that students follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by contacting them immediately to support.
- Following the correct procedures by notifying the ICT Manager if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.

- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of ‘it could happen here’.

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school’s ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

Visitors and members of the community who use the school’s ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Teaching and Learning

4.1 Why is internet use important?

Internet use is part of the statutory curriculum and a necessary tool for learning. The Internet is a part of everyday life for education, business, and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience whilst on the school site. Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school’s management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

4.2 Inclusion of AI tools, Esports and collaborative platforms

Online safety education will explicitly cover the use of artificial intelligence tools (e.g., ChatGPT, Copilot), Esports platforms, and collaborative learning environments (e.g., Microsoft Teams, Academy 21, Google Workspace). Students will be taught:

- How to use these tools responsibly and in line with the school's Online Safety Policy.
- The risks associated with misuse, including exposure to inappropriate content, plagiarism, or unsafe communication.
- The importance of critical evaluation of AI generated content and respectful participation in collaborative platforms.
- Safe behaviour in the Esports suite, including adherence to cabined accounts and supervised sessions.

These areas will be embedded across the curriculum and reinforced through tutor time, RHSE and Esports lessons.

4.3 How does internet use benefit education?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries.
- educational and cultural exchanges between students worldwide.
- vocational, social and leisure use in libraries, clubs and at home.
- access to experts in many fields for students and staff.
- collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- access to learning wherever and whenever convenient.

4.4 How can internet use enhance learning?

The school's Internet access will be designed to enhance and extend education. Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The schools will ensure that the copying and subsequent use of Internet derived materials by staff and students complies with copyright law.

- Access levels will be reviewed to reflect the curriculum requirements and age of students.
- Staff should guide students to online activities that will support the learning outcomes planned for the students' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

4.5 How will students learn how to evaluate internet content?

Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The evaluation of online materials is a part of teaching/learning in every subject.

4.6 Artificial Intelligence (AI) and online safety

Educational use and evaluation of AI content

Students will be taught to critically evaluate content produced by artificial intelligence tools such as ChatGPT, Copilot, and other generative platforms. This training will include:

- Understanding that AI generated information may contain inaccuracies, bias, or incomplete perspectives.
- Checking AI outputs against trusted sources and verifying accuracy before use in schoolwork.
- Recognising the importance of citing sources correctly and not presenting AI generated text as original research.
- Developing awareness of ethical considerations, including plagiarism, data privacy, and responsible use of emerging technologies.

The evaluation of AI generated materials will be embedded across subjects, ensuring students can use these tools responsibly and effectively.

Safeguarding risks and AI usage policy

Generative AI tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

The Lionheart School recognises that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone’s likeness.

The Lionheart School will treat any use of AI to bully students very seriously, in line with our behaviour policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, students and staff.

4.7 Remote learning platforms (Microsoft Teams and Academy 21)

The school provides access to remote learning platforms, including Microsoft Teams and Academy 21, to support education both in school and at home. Students are expected to use these platforms responsibly and in line with the school’s Online Safety Policy.

- Students must log in using their school accounts only.
- Cameras and microphones should be used appropriately and only when directed by teaching staff.
- Chat functions must be used respectfully and only for educational purposes.
- Recording or capturing lessons is strictly prohibited unless explicit permission is granted by the teacher.
- Any misuse of these platforms will be treated as a breach of the Online Safety Policy and may result in restricted access or disciplinary action.

The school recognises the importance of balanced screen time during remote learning. Students will be advised to take regular breaks, follow the 20-20-20 rule (every 20 minutes, look at something twenty feet away for 20 seconds), and avoid excessive use of devices outside scheduled lessons. Parents will be provided with guidance to help manage screen time at home.

4.8 Esports suite use

The school provides an Esports suite to enhance learning, teamwork, and digital skills. Use of this facility is subject to strict safeguarding measures.

- Only PEGI 12-rated games approved by the school may be accessed. PEGI 16-rated will only be available to those 16+ and considered on a case by case basis. Games will not be downloaded with unsuitable PEGI ratings if computers are being shared by students.
- Downloads and installation of software are restricted to the Digital Lead; students are not permitted to install or modify software.
- Accounts are cabined: external chat and communication features are disabled to protect students.
- Students must not attempt to enable or bypass restrictions on accounts or devices.
- All Esports activities must be supervised by staff and conducted in a respectful and inclusive manner.
- Misuse of the Esports suite, including attempts to access unapproved games or enable external communication, will be treated as a breach of the Online Safety Policy.

To promote wellbeing, students will be encouraged to maintain a healthy balance between Esports activities and other learning. Staff will monitor session lengths and ensure breaks are scheduled. Guidance on screen time limits will be shared with students and parents to support responsible use.

4.9 Rules for video conferencing platforms

When using video conferencing platforms such as Microsoft Teams, and Zoom if required, students and staff must follow clear rules to ensure safety and professionalism:

- Access must be through school issued accounts only.
- Students should join sessions punctually and be prepared to learn.
- Cameras and microphones should be used only when directed by teaching staff, with appropriate backgrounds and surroundings.
- Chat functions must be used respectfully and solely for educational purposes.
- Recording, capturing, or sharing lessons is strictly prohibited unless explicit permission is granted by the teacher.
- The same standards of behaviour apply online as in the physical classroom.
- Staff must supervise sessions and report any misuse in line with the school's escalation process.

5. Cyberbullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

5.2 Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Cyber-bullying will be discussed in their tutor groups.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

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

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6. Managing Information Systems

6.1 How will information systems security be maintained?

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working

day will affect the service that others receive.

- Users must take responsibility for their network use.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in students' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- Data Swift will review system capacity regularly.

6.2 Cybersecurity measures

To strengthen the security of school information systems and protect sensitive data, the following measures will be implemented:

- **Phishing-resistant Multi-Factor Authentication (MFA):** Access to staff devices and one-to-one student devices will be through biometric or PIN. Such devices will sign in to Microsoft 365 accounts through device-bound, FIDO2 passkeys. On Windows devices, this will be via Windows Hello. On iOS or Android devices, this will be via Microsoft Authenticator.
- **Shared student devices:** Access to shared student devices will be through sign-in to a Microsoft 365 account with a Strong Password (a "Strong Password" is defined to be a password conforming to the "three random words" format recommended by the National Cyber Security Centre). There will be no requirement to change the password upon an expiry date. Access to such accounts will be restricted to devices managed through the school's Microsoft 365 tenancy.
- **Access to online services:** Where possible, Microsoft 365 Single Sign-On (SSO) will be used to access online services. In all other cases, a Strong Password and Multi-Factor Authentication will be required.

- **Encryption:** Sensitive data, including student records and safeguarding information, will be encrypted both in transit and at rest to ensure confidentiality and compliance with UK GDPR.
- **Regular Security Audits:** The school will conduct periodic audits of cybersecurity measures and update protocols as needed.

6.3 Device Management and Security Audits

To ensure the security of school owned devices and protect sensitive data:

- **Device Management Policy:**
    - All school owned devices (including laptops and tablets) must be enrolled in the school's device management system.
    - Lost or stolen devices must be reported immediately to the ICT team and the Designated Safeguarding Lead. Remote wipe capability will be enabled to protect data.
- **Regular Security Audits:**
    - The school will conduct regular penetration testing and/or external security audits to identify vulnerabilities and ensure compliance with cybersecurity best practices.
    - Findings from audits will be documented and addressed promptly as part of the school's continuous improvement process.

6.4 How will Email be managed?

- 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.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- Teams chat or other messaging platforms for inappropriate communication is prohibited.
- Schools may have a dedicated email for reporting wellbeing and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team.
- Staff should only use school email accounts and Teams to communicate with students as approved by the Senior Leadership Team.

- Staff to student communication via teams must only take place between school accounts and must always remain professional.
- Staff should not use personal email accounts during school hours or for professional purposes.

6.5 How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or students' personal information must not be published.

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

6.6 Can students images or work be published?

- Images of students will be chosen carefully to ensure they do not include any identifiable or sensitive information.
- Students' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of students are electronically published.

6.7 How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites. Social networking platforms and online forums will be unavailable to students. Although access is limited on site and on home use laptops, students will still be provided guidance on appropriate use.

- Students will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests, and clubs etc.
- Students should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- If personal publishing is to be used with students, then it must use age appropriate site suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted

communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.

- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful, or defamatory.

6.8 How will filtering be managed?

If staff or students discover unsuitable sites, the URL must be reported to the Designated Safeguard Lead. The school's broadband access will include filtering appropriate to the age and maturity of students.

- 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 must be reported to appropriate agencies such as CEOP.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students.
- Filtering and monitoring systems will be applied to all school-owned devices, including laptops used at home, wherever technically possible. This ensures that students remain protected when accessing the internet outside of school premises. Parents and carers will be informed of these safeguards and encouraged to support responsible use at home.

6.9 How can emerging technologies be managed?

Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.

Formal approval and ongoing evaluation of emerging technologies:

To ensure safe and effective integration of innovative technologies, the school will implement the following measures:

- **Formal Approval Process:** Any new digital tool, platform, or technology (including AI tools and Esports software) must undergo a formal approval process before use. This process will include:
    - A risk assessment covering safeguarding, data protection, and educational value.
    - Review and sign off by the Designated Safeguarding Lead and Senior Leadership Team.
- **Ongoing Evaluation:** Approved technologies will be subject to regular evaluation to ensure continued compliance with safeguarding standards and educational objectives. This includes:
    - Monitoring usage and impact on student wellbeing and learning.
    - Reviewing risks associated with updates or new features.

  - Updating staff and student training as technologies evolve.

- **Documentation:** All approvals and evaluations will be logged and retained as part of the school's ICT governance records.

6.10 How should personal data be protected?

The UK GDPR and Data Protection Act 2018 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles),
which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

1. Processed fairly and lawfully
2. Processed for specified purposes
3. Adequate, relevant, and not excessive
4. Accurate and up to date
5. Held no longer than is necessary
6. Processed in line with individual's rights
7. Kept secure
8. Transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred, and made available according to the UK GDPR and Data Protection Act 2018.

6.11 Esports accounts – cabined and monitored

All Esports accounts provided by the school are cabined to ensure student safety. This means that external chat, friend requests, and communication features are disabled. Accounts are monitored by staff and the Digital Lead to ensure compliance with the school's Online Safety Policy.

- Students must not attempt to enable or bypass restrictions on Esports accounts.
- Any attempt to access external communication features or unapproved content will be treated as a breach of the Online Safety Policy.
- Monitoring of Esports accounts will be carried out regularly to safeguard students and ensure responsible use.
- Parents and carers will be informed of these restrictions to support safe use and understanding of the Esports suite.

7. Policy Decisions

7.1 How will internet access be authorised?

The school will maintain a current record of all staff and students who are granted access to the school's electronic communications. For some students access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials. Other students must apply for Internet access individually by agreeing to comply with the Online Safety Rules. Parents will be asked to sign a consent form for student access during induction.

- Parents will be informed that students will be provided with supervised Internet access.

7.1.1 Rules for Esports participation

Participation in the school's Esports programme is subject to clear rules designed to safeguard students and ensure responsible use:

- Students must sign an Esports Acceptable Use Agreement, countersigned by parents/carers, before taking part.
- All Esports sessions must be supervised by staff at all times.
- Only school-approved games (PEGI 12 or below) may be accessed.
- Students must use school issued accounts; personal accounts are not permitted.
- Any breach of the Esports Acceptable Use Agreement may result in suspension from Esports activities and further disciplinary action in line with the school's behaviour policy.

7.1.2 Parental consent for home laptop use

Students may only take school-owned laptops home once explicit parental consent has been obtained. Parents/carers must sign a Home Laptop Use Agreement confirming that:

- They understand filtering and monitoring systems will be applied to school laptops wherever technically possible.
- They will supervise their child's use of the device at home and ensure it is used responsibly.
- They accept responsibility for supporting the school's Online Safety Policy outside of school premises.
- They will report any concerns about inappropriate use to the school's Designated Safeguarding Lead.

Without signed parental consent, students will not be authorised to use school laptops at home.

7.2 How will risks be assessed

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. Neither the school nor IOW Council can accept liability for the material accessed, or any consequences resulting from Internet use. The school recognises that students may use school laptops at home. Filtering and monitoring will extend to these devices where possible, and parents/carers are expected to supervise use in line with the school's Online Safety Policy.

- 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.

Risk assessments and safeguarding measures will follow the principles outlined in KCSIE and the Prevent Duty, ensuring that online activity does not expose students to radicalisation, extremism, or other safeguarding risks.

7.2.1 Risks of gaming platforms

The school recognises that while Esports accounts used within the school are cabined and monitored, students may also access personal gaming accounts at home or outside school. These platforms may expose students to risks including:

- Unsupervised communication with strangers through chat or messaging functions.
- Exposure to inappropriate or harmful content.
- Pressure to share personal information or engage in unsafe behaviour.
- Excessive use impacting wellbeing, balance, and academic progress.

Students will be educated about these risks as part of the Online Safety curriculum, and parents/carers will be provided with guidance to support safe gaming practices at home.

7.2.2 Risks of AI misuse

The school recognises that artificial intelligence tools (e.g., ChatGPT, Copilot, and other generative platforms) present specific risks if misused. These risks include:

- **Plagiarism:** Students may attempt to present AI-generated work as their own without proper attribution.
- **Misinformation:** AI outputs may contain inaccuracies, bias, or fabricated information that could mislead students.
- **Over reliance:** Students may depend on AI tools without developing independent research and critical thinking skills.
- **Ethical concerns:** Misuse of AI may undermine academic integrity and responsible digital citizenship.

Students will be educated on these risks through online safety lessons, and staff will receive training to support responsible use of AI in education. Parents/carers will also be provided with guidance to help monitor and support safe use at home.

7.3 How will online safety complaints be handled?

Any complaint about staff misuse must be referred to the headteacher. All Online Safety complaints and incidents will be recorded by the school — including any actions taken.

- Any issues (including sanctions) will be dealt with according to the school's

  disciplinary and child protection procedures.
- Parents and students will work in partnership with staff to resolve issues.

7.3.1 Escalation process for online safety incidents

To ensure timely and transparent handling of online safety concerns, the following process will apply to all incidents (excluding Esports-specific cases, which follow section 6.3a):

- **Step 1 – Immediate Reporting:**
  - Any staff member who becomes aware of an online safety concern must report it to the Designated Safeguarding Lead (DSL) within 24 hours.
  - Students and parents should be encouraged to report concerns promptly to a member of staff.
- **Step 2 – Initial Assessment:**
  - The DSL will review the concern within one working day and determine whether immediate action is required (e.g., restricting access, safeguarding intervention).
- **Step 3 – Investigation:**
  - The DSL, supported by the Senior Leadership Team, will investigate the incident. This may include reviewing logs, interviewing involved parties, and gathering evidence.
  - Investigations should be completed within five working days unless external agencies are involved.
- **Step 4 – Communication of Outcomes:**
  - Parents/carers will be informed of the incident and the outcome of the investigation.
  - Where appropriate, students will receive feedback and guidance to prevent recurrence.
- **Step 5 – Recording and Review:**
  - All incidents will be logged in the school's safeguarding system.
  - Patterns or recurring issues will be reviewed during the annual Online Safety Policy audit.

- **Step 6 – External Referral:**
  - If the incident involves illegal activity or serious safeguarding concerns, the school will contact relevant agencies (e.g., CEOP, police) immediately.

7.3.2 Escalation process for Esports-related incidents

Any incidents arising from the use of the school's Esports suite will follow a clear escalation process to ensure student safety and accountability:

- **Step 1 – Immediate Response:** Staff supervising the Esports suite will intervene to stop inappropriate behaviour and record the incident.
- **Step 2 – Reporting:** The incident will be reported to the Digital Lead and the Designated Safeguarding Lead (DSL).
- **Step 3 – Investigation:** Logs of account activity will be reviewed, and students involved will be spoken to. Witness statements may be taken where appropriate.
- **Step 4 – Parental Notification:** Parents/carers will be informed of the incident and any initial findings.
- **Step 5 – Sanctions:** Depending on severity, sanctions may include temporary suspension of Esports access, restricted account use, or wider disciplinary measures in line with the school's behaviour policy.
- **Step 6 – External Referral:** If the incident involves illegal activity or safeguarding concerns, the school will contact relevant external agencies (e.g., CEOP, police).

All Esports related incidents will be logged and monitored to identify patterns and ensure ongoing safety.

7.4 How is the interne used across the community?

The school will be sensitive to Internet related issues experienced by students out of school, e.g. social networking sites and offer appropriate advice.

7.5 How will cyberbullying be managed

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying. There will be clear procedures in place to support anyone affected by Cyberbullying.

- All incidents of cyberbullying reported to the school will be recorded.
- Students, staff, and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying, and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

This section should be read in conjunction with the school's Child Protection Policy and Anti-Bullying Policy, which outline detailed procedures for safeguarding and supporting students affected by bullying or online harm. Any incidents involving potential harm or abuse will follow the escalation process set out in the Child Protection Policy, and sanctions for bullying will align with the Anti-Bullying Policy.

8. Communication Policy

8.1 How will the policy be introduced to students?

All users will be informed that network and Internet use will be monitored.

- Student instruction in responsible and safe use should precede Internet access.
- An Online Safety module will be included in the RSHE and/or Digital programmes covering both safe school and home use.
- Online Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where students are vulnerable.

8.1.1 Online safety training for gaming and Esports

Students will receive explicit online safety training covering gaming and Esports upon their initial session with staff. This training will include:

- Understanding age ratings (PEGI) and why they matter.
- Safe and respectful behaviour when playing games in the school's Esports suite.
- Risks associated with online gaming, including chat functions, external communication, and exposure to inappropriate content.
- Clear guidance on the restrictions in place (cabined accounts, disabled chat, supervised sessions) and the importance of not attempting to bypass them.
- Encouragement of healthy balance between gaming, learning, and wellbeing.

This training will be reinforced regularly through Esports lessons and will be revisited when students transition between key stages.

8.1.2 Remote learning etiquette

Students will be provided with clear guidance on appropriate behaviour during remote learning sessions delivered via Microsoft Teams and Academy 21. This guidance will include:

- Logging in with school-issued accounts only.
- Joining lessons punctually and prepared to learn.
- Using cameras and microphones only when directed by teaching staff and ensuring backgrounds and surroundings are appropriate.
- Using chat functions respectfully and only for educational purposes.
- Not recording, capturing, or sharing lessons without explicit permission from the teacher.
- Following the same standards of behaviour online as are expected in the classroom.

Remote learning etiquette will be reinforced regularly through online safety, tutor time and revisited when students transition between key stages.

8.2 How will the policy be discussed with staff?

The Online Safety Policy will be formally provided to and discussed with all members of staff. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- All staff will receive a copy of Staff Acceptable Use of ICT.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.
- Staff training will include awareness of statutory guidance such as KCSIE and the Prevent Duty, ensuring they understand their responsibilities in identifying and reporting online risks, including radicalisation.
- All staff will receive training on cybersecurity best practices, including password management, multi-factor authentication, phishing awareness, and safe handling of sensitive data. This training will be refreshed regularly and incorporated into wider safeguarding and ICT training programmes.

8.2.1 Training on Esports supervision

Staff responsible for supervising the school’s Esports suite will receive specific training to ensure student safety and responsible use. This training will include:

- Understanding the restrictions in place (cabined accounts, disabled chat, approved PEGI 12 games).
- Monitoring student behaviour during Esports sessions and intervening promptly when necessary.
- Recording and reporting incidents in line with the school’s escalation process.
- Promoting respectful teamwork and inclusion within Esports activities.

- Recognising potential risks associated with online gaming and supporting students in managing these responsibly.

Training will be refreshed regularly and incorporated into wider staff safeguarding and Digital training programmes.

8.2.2 Training on AI tools in education

Staff will receive training on the safe and effective use of artificial intelligence tools (e.g., ChatGPT, Copilot, and other generative platforms) within teaching and learning. This training will include:

- Understanding the capabilities and limitations of AI tools.
- Recognising risks such as bias, inaccuracies, and plagiarism.
- Supporting students in critically evaluating AI generated content.
- Embedding responsible use of AI into classroom practice and curriculum delivery.
- Ensuring compliance with safeguarding, data protection, and academic integrity requirements.

Training will be refreshed regularly and incorporated into wider staff development programmes to ensure confidence in guiding students' use of AI.

8.2.3 Staff responsibilities and reporting obligations

All staff have a duty to uphold this Online Safety Policy and safeguard students when using technology. This includes:

- **Reporting Obligations:**
  - Staff must immediately report any suspected misuse of technology, breaches of this policy, or safeguarding concerns (including inappropriate online behaviour) to the Designated Safeguarding Lead (DSL).
  - Failure to report concerns may be treated as a safeguarding breach.
- **Professional Conduct:**
  - Staff must use school systems responsibly and in line with the Staff Acceptable Use Agreement.
  - Communication with students must remain professional and occur only through approved school platforms.
- **Disciplinary Consequences:**
  - Breaches of this policy by staff will be investigated in line with the school's disciplinary procedures.

  - Serious breaches, including failure to report safeguarding concerns or deliberate misuse of technology, may result in formal disciplinary action up to and including dismissal.

8.3 How will parents support be enlisted?

Parents' attention will be drawn to the School Online Policy on the school website.

- Parents will be requested to sign an Acceptable Use of ICT Agreement upon induction.
- Information and guidance for parents on Online Safety will be made available to parents in a variety of formats.

8.4 Guidance for monitoring home laptop use

The school recognises that students may use school owned laptops at home for homework, online lessons, and research. To ensure safe and responsible use outside of school premises:

- Filtering and monitoring systems will be applied to school laptops wherever technically possible. (see also Section 5.6 – Filtering).
- Parents and carers are expected to supervise their child's use of the device, ensuring it is used in line with the school's Online Safety Policy.
- Students must not attempt to disable or bypass safety settings on school laptops.
- Any concerns about inappropriate use at home should be reported to the school's Designated Safeguarding Lead.
- Guidance and support will be provided to parents to help them encourage safe and balanced use of technology at home.

9. Training

9.1 Staff, governors and volunteers

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

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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages

    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

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

9.2 Students

All students will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Students will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

10. Monitoring Arrangements

- The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in the appendices.
- This policy will be reviewed every year by the DSL, Digital Lead and ICT Manager. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

11. Appendices

Appendix 1 – Online Safety Training Needs Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for students and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2 – KS4 Acceptable Use Agreement (Students and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET:

AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for students using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3 – Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of students without checking with teachers first
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a student informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4 – Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 5 – Esports Acceptable Use Agreement

Esports Acceptable Use Agreement

This agreement sets out the rules for students participating in the school's Esports programme. It ensures that gaming activities are safe, respectful, and educational.

Rules for Students

- **Signed Agreement**: You and your parent/carer must sign this document before taking part.
- **Supervised Sessions**: All Esports activities will be supervised by staff.
- **Approved Games Only**: You may only play school approved games (PEGI 12 or below).
- **School Accounts**: You must use the school issued Esports account. Personal accounts are not permitted.
- **Cabined Accounts**: External chat, friend requests, and downloads are disabled for safety. Do not attempt to bypass these restrictions.
- **Respectful Behaviour**: Treat teammates, opponents, and staff with respect at all times.
- **No Modifications**: Do not install, modify, or delete software on Esports suite devices.
- **Consequences**: Breaches of these rules may result in suspension from Esports activities and further disciplinary action.

Responsibilities of Parents/Carers

- Support your child in following these rules.
- Encourage healthy balance between gaming, schoolwork, and wellbeing.
- Report any concerns about Esports participation to school staff.

Agreement

By signing below, you confirm that you understand and agree to follow the rules of the school's Esports programme.

Student Name	
Student Signature	
Date	
Digital Lead	
Signature	
Date	

Appendix 6 – The Lion's Den – Code of Conduct

The Lion's Den – Code of Conduct

At The Lionheart School, we are committed to creating a safe, respectful, and positive environment for all players in our Esports suite. Our expectations align with the British Esports Association Code of Conduct, and we uphold these standards to ensure fairness and wellbeing for everyone.

If any player behaves in a way that contradicts these expectations, staff will address the situation promptly and involve parents or guardians where necessary. Continued breaches may result in suspension or permanent removal from the Esports suite to protect the welfare of other players and staff.

Players (and, where appropriate, Staff) agree to:

✓ Respect the Equipment

Take care of all Esports suite equipment and report any damage or issues to staff immediately.

✓ Play Fair

Follow the rules of the platform, the games, and any competitions or events.

✓ Show Good Sportsmanship

Be respectful whether you win or lose.

✓ Treat Others with Respect

Interact with others as you would like to be treated yourself.

✓ Be Kind and Fair

Recognise that everyone has different levels of skill and ability.

✓ Remember People Online Are Real

Your words and actions can affect others—choose them carefully.

✓ Set a Positive Example

Demonstrate good behaviour at all times.

✓ Support and Encourage

Help your teammates and others to succeed.

✓ Speak Out Against Harmful Behaviour

Do not tolerate bullying, harassment, or abuse.

✓ Listen and Reflect

If told your words or actions are harmful, stop and reconsider.

✓ Respect Different Views

Even if you disagree, remain courteous.

✓ Report Concerns

Inform staff about any bullying, cheating, or inappropriate behaviour during games, events or competitions.

✓ Avoid Exploits and Disrespectful Actions

Do not use in game bugs or display behaviour that could harm others.

✓ Play Honestly

Do not collude or coerce other teams to force a specific outcome