The Olympus Academy Trust
Online Safety and Acceptable Usage Policy

Document Summary

Document Owner:	Director of IT
Version:	**3.1**
Document Status:	**Approved**
Date Last Approved:	27th November 2025
Date of Next Review:	27th November 2026
Review Frequency:	Annually
Owner: (Olympus or School)	Olympus Academy Trust
Governing Committee:	Audit and Risk Committee
Statutory or Optional policy:	Optional
Appendices:	Appendix A - Learner Acceptable Use Agreement (for KS2 – KS5 learners) Appendix B - Learner Acceptable Use Agreement (for KS1 learners) Appendix C - Staff, Members, Trustees, Governors (and other Volunteers) Acceptable Use Agreement Appendix D - Parent/Carer Acceptable Use Agreement Appendix E - Acceptable Use Agreement for Community Users Appendix F - ICT Access Denial Form Appendix G - Technical Security Policy (including filtering and authentication) Appendix H - Loaned Digital Device / Laptop Acceptable Use Agreement
On Trust Website?	Yes
On School Websites?	Yes
Consulted with JCNC. Y/N or not applicable	n/a

Amendment History

Version	Amendment Date	Author	Amendment Summary
0.1	16/09/22	THi	• New Policy
1.0	23rd November 22	THi	• Policy has been circulated to all heads for comments which have been incorporated into the policy. Policy will be given to Audit and Risk for approval.
1.0	29th November 22	Policy Coordinator	• Policy has been approved by Audit & Risk Committee (with the proviso that BTEA is removed from the table on page 30. • Policy issued.
2.0	24th October 2023	Director of IT	• Minor amendment - Incorrect email addresses amended.
2.1	30th November 2023	Policy Coordinator	• Approved by Audit and Risk Committee
3	20th October 2025	Head of Business Operations and Executive Office Manager	• Significant changes throughout the document to meet GDPR and Cyber Security requirements
3.1	27th November 2025	Policy coordinator	• Approved by ARC on 27th November

1. **Scope of the Policy**
   This Online Safety and Acceptable Usage Policy outlines the commitment of the Olympus Academy Trust to safeguard members of our school community online in accordance with statutory guidance and best practice.

   This policy applies to all members of the school community (including staff, Governors, Trustees, Members, learners, volunteers, parents and carers, visitors and community users) who have access to and are users of school digital systems, both in and out of the schools. It also applies to the use of personal digital technology on school sites (where allowed).

   The Olympus Academy Trust will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

2. Purpose of the Policy

Our Trust aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers, members, governors and trustees.
- Identify and support groups of learners 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 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, fake news, 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 them 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
- Relationships and sex education
- Searching, screening and confiscation
- Generative artificial intelligence (AI) in education
- Generative AI: product safety expectations

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 learners' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.
This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees has overall responsibility for monitoring this policy and holding the Chief Executive Officer to account for its implementation.

The Board of Trustees will oversee the co-ordination of regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Trustees, Members and Governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Trust's ICT systems and the internet (Appendix C)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some learners 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 Chief Executive Officer (CEO)

The CEO (and/or his nominated member of the senior leadership team) will:

- Review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the trust and its schools 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;
  - Ensure that online safety is a running and interrelated theme while devising and implementing the trust-wide approach to safeguarding and related policies and/or procedures
  - Review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
  - Ensure that the workforce understand this policy, and that it is being implemented consistently throughout the trust.
  - Ensure the workforce undertakes online safety training as part of child protection and safeguarding training, and ensure they understand the expectations, roles and responsibilities around filtering and monitoring.

3.3 Headteachers

The Headteacher is responsible for:

- Working with the IT department to make sure the appropriate systems and processes are in place
- Ensuring that the workforce understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring that the Trust Online Safety Policy is published and reviewed regularly.
- Ensuring the workforce undertakes online safety training as part of child protection and safeguarding training, and ensure they understand the expectations, roles and responsibilities around filtering and monitoring.
- Ensuring the workforce complete the National Cyber Security Centre training for school staff at least annually
- Ensuring 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.
- Ensuring that teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some learners 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 contextualized approach may often be more suitable
- Working with the DSL, ensuring that regular checks and audits of the filtering and monitoring systems take place, are recorded and actions are followed.
- Reporting to governors/trustees on the effectiveness of online safety and the filtering and monitoring systems.

  Review monthly filtering and monitoring reports regularly alongside the governing body, DSLs and appropriate Trust staff

3.4 Trust Director of SEND, Inclusion & Vulnerable Groups

- The Trust Director of Safeguarding oversees the work of school Designated Safeguarding Leads and provides support to them with online safety. In particular this postholder regularly reviews and updates the blocked website categories, and informs the IT Department of any required changes to the enforcement policy.

3.4 Designated Safeguarding Leads (DSLs)

Details of the school's designated safeguarding lead (DSL) and deputy/deputies 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 ensuring that staff understand this policy and that it is implemented consistently throughout the school
- Working with the Headteacher, Trust IT team 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 child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy

- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or School Improvement Committee

This list is not intended to be exhaustive.

3.5 The Director of IT

The Director of IT is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure learners are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Update the enforcement policy in line with guidance from the Trust Director of SEND, Inclusion & Vulnerable Groups
- Ensuring that the school's IT 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 on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that IT systems are in place to monitor and provide reporting to the appropriate Designated Safeguarding Leads (DSL).

This list is not intended to be exhaustive.

3.6 All staff and volunteers

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 Trust's IT systems and the internet (Appendix C), and ensuring that learners follow the school's terms on acceptable use (Appendices A and B)
- Working with DSLs to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring 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.

3.7 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (Appendices A and B) and signing to confirm this (Appendix D)

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent resource sheet - Childnet International

3.8 Community Users

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix E).

4. Educating learners about online safety

Learners will be taught about online safety as part of the curriculum:

All schools must teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, learners will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Learners in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, learners will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, learners will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns

Learners in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, learners will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some learners with SEND.

5. Educating parents about online safety

Trust schools will raise parents' awareness of internet safety in letters or other communications home, and in information via websites. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

Schools will let parents know:

- What systems the school uses to filter and monitor online use
- An overview of what their children are being asked to do online, including the type of sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 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.)

6.2 Preventing and addressing cyber-bullying

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

Schools will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners, as part of safeguarding training (see section 11 for more detail).

Schools send information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

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

DSLs will report incidents 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.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or learners, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, the authorised staff member will:

- Assess how urgent the search is, and consider the risk to other learners and staff
- Explain to the learner why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the learner's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL/Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The learner and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of learners will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- School behaviour policies

Any complaints about searching for or deleting inappropriate images or files on learners' electronic devices will be dealt with through the Trust's complaints procedure.

7. **Artificial intelligence (AI)**

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, learners and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Olympus Academy Trust recognises that AI has many uses to help learners 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 Olympus Academy Trust will treat any use of AI to bully learners in line with our anti-bullying/behaviour policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school and or trust. Please notify your IT Department or the Trust GDPR Leads if you would like to use any new software/websites.

As AI capabilities are increasingly integrated into our everyday systems, the Trust is dedicated to safeguarding all its stakeholders. Consequently, the Trust reserves the right to monitor and review AI prompts, interactions, and general usage. Anyone signing into Office 365 with their Trust credentials (email address), regardless of whether it's on their personal device or a Trust device, will be subject to monitoring and reporting. Using a Trust email address in any online system places all subsequent interactions within the Trust IT ecosystem and associated monitoring systems

8. Acceptable use of the internet in schools

All learners, parents, staff, volunteers, Governors, Members and Trustees are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices A to E). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by learners, staff, volunteers, Governors, Members, Trustees and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices A to E.

9. Mobile devices in school

Secondary Phase Learners

- All phones and other mobile devices etc. should be turned off and placed in bags/locker as soon as learners arrive in school. They should not be taken out or used in the school building without permission from a staff member.
- Learners may not take any images or videos of learners or members of staff without permission.
- Learners must never post images of staff or learners in school on any website, social networking site or similar and should not write about them in an offensive or slanderous manner.

Primary Phase Learners

Primary phase children should not bring mobile phones into school, unless in exceptional circumstances and with prior agreement with the teacher or Headteacher. If permission is granted, the device should be kept in a locked location in the school office and returned at the end of the school day.

Post 16 Learners

Post 16 learners are permitted to bring mobile devices into school and to keep them on their person as long as they do not disrupt learning, as judged by the member of staff in charge. Any misuse of this privilege may result in it being withdrawn.

Staff, Governors, Trustees, Members or other Visitors

- Staff should not take pictures of any learner or store any information relating to learners on their personal mobile device.
- Mobile phones should be on silent/vibrate and kept in a bag or pocket wherever possible on the school site and while learners are present.

Misuse of any personal device will be dealt with via the relevant policy for learners or staff.

10. Staff using work devices outside of schools

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 12 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring any storage devices (e.g USB memory sticks) are encrypted – this means if the device is lost or stolen, no one can access the files stored on the drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Ensuring that updates are not unduly delayed
- Never leaving your laptop or device unattended or leaving a laptop in a car

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix C.

Work devices must be used solely for work activities. This applies to web browsing or accessing a personal email account.

If staff have any concerns over the security of their device, they must seek advice from the IT Team.

Further information can be found in the Trust Technical Security Policy (Appendix G).

11. Social Media – Protecting Professional Identity

The Olympus Academy Trust has a duty of care to provide a safe learning environment for learners and staff. The Trust could be held responsible, indirectly, for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the Trust liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

10.1 The Trust provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

10.2 Trust staff should ensure that:

- No reference should be made in social media to learners, parents/carers or Trust staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- They do not accept “friend requests” from learners

10.3 When official school/Trust social media accounts are established there should be:

- A process for approval by senior/executive leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under Trust disciplinary procedures

10.4 Personal Use:

- If members of staff post or comment on social media, including indicative comments such as ‘likes’ or sharing, that brings the Trust into disrepute then this will be addressed as if it had taken place at your place of work. You may also be asked to remove the online content that is not in line with this policy. This is also the case for any social media usage that is found to cause offence to, discriminate against, defame or disparage any other member of staff, learner or parent/carer or other Trust or School stakeholder.
- Staff should also be very cautious in sharing information that may contain personal, sensitive, or confidential matters relating to the Trust or individuals within it. This could compromise the safety of individuals, break GDPR laws or damage the Trust’s reputation. All social media posts should continue to follow the Trust’s policies.
- Staff should not provide references for other individuals through social media sites as references can be attributed to the organisation and create legal liability for the author and the organisation.
- Staff should, if affiliation with the Trust is obvious, make it clear that opinions presented are those of the individual and not the Trust. However, staff must be aware that stating that the opinion presented in social media is one’s own does not automatically provide license to use Social Media in a way that contravenes the requirements outlined above. Staff still represent the Trust and/or school. Staff must not use social media to present the opinions of the Trust without having gained express permission from your Line Manager.

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Inappropriate social media use (including but not limited to context of an abusive, harassment, bullying, abuse of protected characteristics or sexual nature) will lead to disciplinary action
- The Trust permits reasonable and appropriate access to private social media sites

10.5 Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

10.6 The school's/Trust's use of social media for professional purposes will be checked regularly by the Trust Director of IT and the Trust Director of Safeguarding to ensure compliance with the school policies.

11. How schools will respond to issues of misuse

Where a learner misuses the Trust's IT systems or internet, schools will follow the procedures set out in their behaviour policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

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, online training 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, 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 learners can recognise dangers and risks in online activity and can weigh up the risks

- Develop the ability to influence learners to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy/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.

Filtering & Monitoring
What is filtering and monitoring?
Filtering and monitoring systems are used to keep learners safe when using our school's IT system.
Filtering is the safety measure designed to restrict and control the content which can be accessed by staff, learners, volunteers, and visitors. Filtering systems block access to harmful sites and content.
Monitoring concerns the review of user activity on the school's network to promote the safeguarding of staff, learners, volunteers, and visitors. Monitoring systems identify when a user accesses or searches for certain types of harmful content on school/trust devices (it doesn't stop someone accessing it). The school/trust is then alerted to any concerning content so that the school/trust can intervene and respond.

All staff should be clear on:

- The expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their safeguarding training. For example, part of their role may be to monitor what's on learners' screens
- How to report safeguarding and technical concerns, such as if:
  - They witness or suspect unsuitable material has been accessed
  - They are able to access unsuitable material
  - They are teaching topics that could create unusual activity on the filtering logs
  - There is failure in the software or abuse of the system
  - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
  - They notice abbreviations or misspellings that allow access to restricted material
- Senior leaders and all relevant staff need to be aware of and understand:
  - What provisions the trust/school has in place and how to manage these provisions effectively
  - How to escalate concerns when they identify them
- They are also responsible for:
  - Buying-in the filtering and monitoring system for the trust/schools (this is actioned trust-wide as part of our IT strategy).
  - Documenting what is blocked or allowed, and why
  - Reviewing the effectiveness of provision, making sure that incidents are urgently picked up, acted on and outcomes are recorded
  - Overseeing reports
  - Making sure staff are trained appropriately and understand their role
- The DSL should take lead responsibility for online safety, including understanding the filtering and monitoring systems and processes in place – this is part of their role in taking the lead responsibility for safeguarding. This includes overseeing and acting on:
  - Filtering and monitoring reports
  - Safeguarding concerns
  - Checks to filtering and monitoring systems
- Each school should:
  - Identify and assign roles and responsibilities to manage filtering and monitoring systems (this is a function of the executive team)
  - Review filtering and monitoring provision at least annually

- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet your safeguarding needs
- Maintain a record (folder) of all filtering and monitoring checks, audits, training and changes

We have an obligation to put in place suitable Filtering and Monitoring systems. These apply to our devices, whether used on site or off site. Filtering and Monitoring will also apply to personal devices that access our internet connection on the site and to personal devices used at home when accessing the Trust network remotely

Unblocking sites
Staff can request sites to be unblocked. Requests should be emailed to the DSL, Headteacher and/or IT coordinator as applicable to the setting. The request should include the following information:

- Staff name and year group/department:
- Website title and URL/link:
- Year group you want the website unblocked for (if applicable):
- Reason why you want the website unblocked:
- Can we re-block this site after a specific date?

A record of the request will be held with the Filtering and Monitoring Log.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on Arbor & CPOMS.

This policy will be reviewed every year by the Director of IT. At every review, the policy will be shared with Trustees.

14. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policies
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

15. **Diversity, Equity and Inclusion Statement**

We are committed to fostering a diverse, equitable, and inclusive environment where every individual is valued and respected. Our policies reflect our dedication to creating a workplace that embraces differences and promotes fairness. We believe that diversity enriches our organisation and drives innovation, and we strive to ensure that all employees have equal opportunities to succeed and thrive.

APPENDIX A

Learner Acceptable Use Agreement (for KS2 – KS5 learners)

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

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

- Always use the school's IT 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 which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it
- Be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- Only use my own personal devices (mobile phones/USB devices/Smart watches etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

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
- Make large downloads or uploads (without permission from a teacher) that might take up internet capacity and prevent other users from being able to carry out their work.
- Take or distribute images of anyone without their permission.

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

APPENDIX B

Learner Acceptable Use Agreement (for KS1 learners)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

APPENDIX C

Staff, Members, Trustees, Governors (and other Volunteers) Acceptable Use Agreement

I understand that I must use Trust systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that learners receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the Trust will monitor my use of the Trust digital technology and communications systems.
- I understand that if I sign into Office 365 using my Trust credentials, even if using a personal device, all activity will be subject to monitoring and reporting.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I understand that work devices must be used solely for work activities. This applies to web browsing or accessing a personal email account

I will be professional in my communications and actions when using Trust systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the Trust's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the Trust's policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the Olympus Academy Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant Trust policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will 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 not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, except those allowed in the Trust policies.
- I will not disable or cause any damage to Trust equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust's Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not use my personal phone to create a hot-spot to access the internet on my work device instead of using the school internet connection

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of Trust digital technology equipment in school but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment or role in the Trust.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the Trust digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

APPENDIX D

Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

Permission Form

Parent/Carer's Name: _____

Learner Name: _____

Learner School: _____

As the parent/carer of the above learner, I give permission for my son/daughter to have access to the internet and to IT systems at school.

Parent Signature: _____

Either: (KS2 and above)

I know that my child has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Or: (KS1)

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that my child's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

APPENDIX E

Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of Trust digital technologies will be responsible users and stay safe while using these systems and devices
- that Trust systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement
I understand that I must use school/Trust systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.
This agreement will also apply to any personal devices that I bring into the school/Trust:

- I understand that my use of Trust systems and devices will be monitored
- I will not use a personal device that I have brought into a school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, 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 not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school/Trust equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that if I fail to comply with this acceptable use agreement, the Trust has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (on Trust sites and when carrying out communications related to the school/Trust) within these guidelines.

Name: _____ Signed_____ Date_____

APPENDIX F

IT Access Denial Form

Dear parents/carers

It is assumed that parents/carers grant their child the right to access The Trust's network across all Trust schools unless this IT Access Denial Form is signed and returned.

Please be aware that IT is used throughout the Trust in all subjects. Without use of the Trust's network, your child will not be able to access many aspects of the curriculum.

If you DO NOT want your son or daughter to have access to the Trust's IT network, please return this form to reception for the attention of IT Support:

Name of Learner_____

Year_____ Tutor group_____

As the parent or legal guardian of the learner named above, I withdraw permission for my son or daughter to access the Trust's network services indicated above.

I am aware that this will impact on his/her ability to access the curriculum and that progress and attainment may be negatively impacted as a result.

Parent (Guardian) Signature: _____

Date: _____

You will be sent confirmation of receipt of this form. Please contact us if you do not receive confirmation within 10 school days.

APPENDIX G

Technical Security Policy (including filtering and authentication)

Introduction
Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training.
The Olympus Academy Trust (The Trust) will be responsible for ensuring that the network is as safe and secure as is reasonably possible, and that:

- users should only access data to which they have a right to process.
- no user should be able to access another's files (other than that allowed for monitoring and support purposes within school/Trust policies).
- access to personal data is securely controlled in line with the Trust's personal data policy.
- relevant logs are maintained of network access by users, and of their actions whilst connected to systems and services.
- there is effective guidance and training for users.
- there are regular reviews and audits of the safety and security of Trust computer systems.
- there is oversight from senior/executive leaders and these have impact on policy and practice.

Responsibilities
The management of technical security will be the responsibility of the Director of IT.

Technical Security
The Trust will be responsible for ensuring that its infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.
The line management process needs to ensure that the relevant IT staff receive guidance and training so that they will be effective in carrying out their duties:

- Trust technical systems will be managed in ways that ensure that the Trust meets recommended technical requirements.
- there will be regular reviews and audits of the safety and security of Trust technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the Trust systems and data.
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.
- All users will have clearly defined and appropriate access rights to Trust systems and services. The details of the access rights attached to system groups will be documented by the responsible systems/service manager who will liaise with the Technical Director. These will be reviewed at least annually, by the Trust Director of IT

- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Mobile device security and management procedures are in place.
- Technical staff regularly monitor and record the activity of users on the Trust technical systems and users are made aware of this in the acceptable use agreement.
- Remote management tools are used by staff to control workstations and view users activity
- Users report any actual/potential technical incident to the IT Helpdesk who will pass information on to the Director of IT (or other relevant person, as agreed)
- An agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the Trust system
- An agreed policy is in place regarding the downloading of executable files and the installation of programs on Trust devices by users
- The Trust infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data should not be sent over the internet or taken off the school/Trust site unless safely encrypted or otherwise secured.

User Account Security

These statements apply to all users:

- All Trust networks and systems must be protected using secure authentication methods, including strong passwords or multi-factor authentication (MFA).
- Personal passwords and MFA tokens must not be shared with anyone.
- All users will be provided with a user account by the IT team.
- The IT team will run regular maintenance on network user accounts, computer and human, to attempt to catch those that are compromised or dormant/unused.
- All users (adults and learners) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Password requirements:

- Choosing your password:
    - Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords.
    - Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack.
    - Passwords should be easy to remember, but difficult to guess or crack.
- Services that require a shared password (e.g. exam boards) must have that password securely regulated.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the Trust
- Passwords must not include names or any other personal information about the user that might be known by others.
- Passwords must be changed on first login to the system

Learner passwords:

- Users will be required to change their password if it is compromised.
- Learners will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.
- An administrator account password for the Trust systems should also be kept in a secure place e.g. Trust safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- It is good practice that where passwords are used, there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where automatically generated passwords are not possible, then a good password generator should be used by the IT Team to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary and the user should be forced to change their password on the first login.
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use.
- Accounts are to be "locked out" following five successive incorrect log-on attempts, with a minimum wait period of 15 minutes before re-enabling.
- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).
- Wherever possible, Single-sign on solutions (SSO) and with a preference, cloud-based identity management should be used to seamlessly sign users into systems

Training/Awareness:

Members of staff will be made aware of the Trust's password policy:

- at induction
- through the Trust's online safety policy
- through the acceptable use agreement

Learners will be made aware of the Trust's password policy:

- in IT lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person (IT Operations Manager: Service Desk & Users) will ensure that full records are kept of user IDs and requests for password changes

Filtering

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering

system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities

The responsibility for the management of the Trust's filtering policy will be held by the IT Operations Manager: Service Desk & Users. They will manage the school filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to and authorised by the Director of IT
- All users have a responsibility to report immediately to senior/executive leaders any infringements of the Trust's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the IT Team. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

- The Trust maintains and supports the managed filtering service provided by the Internet Service Provider
- The Trust has provided enhanced/differentiated user-level filtering through the use of the Integra filtering programme. (Allowing different filtering levels for different ages/stages and different groups of users – staff/learners etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Director of IT (or other executive leader)
- Mobile devices that access the Trust internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on school/Trust systems
- Any filtering issues should be reported immediately to the filtering provider.

Education/Training/Awareness

Learners will be made aware of the importance of filtering systems through the online safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the acceptable use agreement
- induction training

- staff meetings, briefings, training sessions

Parents and carers will be informed of the school's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletters/websites.

DO NOT send defamatory emails, or use email for harassment or to share protected information with people.

DO NOT pass on virus warnings to other people. Many are hoaxes designed to cause disruption in precisely this way.

DO NOT click on a link in an email and enter any personal information or your password.

DO NOT act on warnings that suggest you delete files from your device. They usually suggest that you delete files essential to the correct working of your computer.

All computer and internet use is recorded in the event that an investigation is required, for example, checking who visited websites or downloaded and/or installed software.

APPENDIX H

LOANED DIGITAL DEVICE / LAPTOP ACCEPTABLE USE AGREEMENT

Parent / Carer Name	
Learner Name	

1 **Purpose**

1.1 This Agreement is intended to ensure:

- All children and young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- School and Trust IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.
- Learners and parents/carers have clear guidelines on appropriate use of the loaned digital device/laptop and the rules that must be followed when it is in use.

1.2 There are two parts to this Agreement. One part for parents/carers and one part for learners/young people. Parents/carers and learners/young people are requested to sign the boxes below to confirm that they have read, understood and agreed to the guidance and rules within this Acceptable Use Policy. ***Both parts must be signed and returned to the school before the loaned device/laptop can be used.***

2. **Rules for using the Loaned Digital Device / Laptop and Keeping Safe Online**

2.1 As the parent/carer of the above child, I give permission for my child to use the digital device provided by The Trust and agree to ensure the rules within the Online Safety and Acceptable Use Policy are followed at all times.

2.2 My child has read, understood and signed an Acceptable Use Agreement and we have discussed the rules within the Online Safety and Acceptable Use Policy.

2.3 I understand that The Trust will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and digital device/laptop. I also understand that The Trust cannot ultimately be held responsible for the nature and content of materials accessed on the internet and digital device/laptop. I understand that I am also responsible for ensuring suitable monitoring and filtering of home internet access.

2.4 I understand that my child's activity on the digital device/laptop will be monitored and that a member of staff from the Trust will contact me if they have concerns about any possible breaches of the Online Safety and Acceptable Use Policy.

2.5 **Computer Misuse Act**

The Computer Misuse Act 1990 introduced three criminal offences: unauthorised access; unauthorised access with intent to commit a serious criminal offence; and unauthorised modification of computer material. Any parent/carer or child identifying or suspecting such activity must report it immediately to the IT Helpdesk.

2.6 **Data Protection Act**

All use of IT systems covered by this policy is also assumed to be covered by the Data Protection Act.

2.7 **Intellectual Property Rights**

Parents/carers and children must be aware of intellectual property rights, such as copyright, design rights and trademarks. Infringement can lead to legal action that may involve criminal proceedings. This warning is particularly pertinent to the use of material available on the internet as the same legal requirements apply.

2.8 **Software Copyright**

The Trust's IT department are responsible for maintaining copies of all software and licences and therefore purchasing all new software. Parents/Carers and children should never purchase, install or download any software or IT services (including hosted ones) themselves irrespective of their value.

2.9 **Unauthorised use of equipment**

The Trust's IT equipment may not be used for unauthorised purposes. This could lead to criminal or fraudulent acts, waste valuable resources, or result in damage to hardware, software or data. This includes inappropriate streaming or downloading of media (e.g. music and video). All internet activity is logged and can be attributable to the user logged in. This device is loaned to a child specifically to support their learning.

2.10 **Home Use of the Internet**

The Trust hopes that you will reinforce the guidance and rules contained in the Child/Young Person's Acceptable Use Agreement when your child uses the loaned digital device/laptop and internet at home and at school. In order to do this we recommend that you:

- Ensure appropriate supervision for the age of your child including supervising all use of the internet by younger users.
- Set appropriate rules for using the IT and the internet safely at home. Your child's school rules could provide a starting point.
- Inform the school if you have concerns that the school could help to address through teaching.

- Ask your child about the sites they are visiting.
- Ensure that family computers are password protected and have robust anti-virus software which is regularly updated.
- Ensure content is appropriately filtered for younger users, most internet providers have this service available.
- Ensure that your child knows that any protection system does not stop all unsafe content and that they need to tell you if they access something inappropriate or get an upsetting message.
- Reassure your child that if they talk to you about a problem they are having on the internet you will not ban them from using it as this will discourage them from telling you.
- Ensure that your child knows not to leave computers logged on with their user name or logged on to sites with personal details entered as others could use them.

2.11 **Keeping Safe**

- The loaned digital device/laptop will not have a password.
- Discuss usernames with children and talk about how to choose them carefully to protect their identity.
- Talk to your child about the information they should keep private in order to prevent them being contacted or traced including full name, address, telephone no., school, places they go to regularly.
- Talk to your child about the need to limit access to their own information by using the safety and privacy features of sites to only give access to people they know and being careful who they add as friends.
- Model safe behaviour in your use of IT.

2.12 **Research and Fun on the internet**

- Children can use the loaned digital device/laptop for educational research but must not use it for recreational purposes such as watching/streaming films or accessing social media.
- Talk to your child about the fact that any information published on the web can be read by anyone and that they should only publish information they would be happy for anyone to read.
- Check information that younger users are publishing on the web before it is posted to ensure that they are not putting themselves at risk.
- Check that your child is old enough for the sites they are using.

2.13 **Communicating**

- Online communicating on the loaned digital device/laptop must be for educational and learning purposes only.
- Discuss the need for young people to be polite to others online and that they should not use bad language or comments which might upset others.
- Discuss the fact that e-mails / messages can be intercepted and forwarded on to anyone (including friends, head teacher or future employer!).
- Ensure that children know they should not open messages if the subject field contains anything offensive or if they do not recognise who it is from and that the safest thing to do is to delete it without opening it.

- Recognise that there is a difference between online friends who you will never meet and real world friends. Talk to your child about their online friends.
- Remind your child that people they talk to online may not be who they seem.
- Remind your child that they must not use the loaned device for communicating on social media for non-educational purposes.

2.14 **Sharing**

- The loaned digital device/laptop must not be used for downloading/streaming films, games, music or any other non-educational content.
- Ensure your child understands that the loan and use of the digital device/laptop is for educational and learning purposes only.
- Ensure your child knows that downloading games and music that is copyrighted without paying for it is illegal.

2.15 **Buying and Selling Online**

- The loaned digital device/laptop must not be used for buying and selling online.
- Help your child to tell the difference between web sites for information and web sites used to sell items.
- Discuss how to recognise commercial uses of the internet e.g. I Tunes, mobile phone downloads, shopping.
- Remind your child that if an offer looks too good to be true it probably is and that they should not respond to unsolicited online offers.
- Remind your child that they should not purchase or download anything that costs money without asking permission and that they should not use someone else's identity to buy things online. The loaned digital device must not be used for this purpose.

2.16 **Problems**

- Ensure your child knows that if they receive an offensive or worrying message / e-mail they should not reply but should save it and tell you.
- Contact the Trust's IT helpdesk for any support queries: Olympus IT Helpdesk.

Signed ..... Date .....

For guidance on how to support your child to stay safe online we recommend looking at the following websites.

Think U Know for Parents - https://www.thinkuknow.co.uk/parents/ provides advice, resources, how to report an issue and online activity packs.

ChildNet - https://www.childnet.com/parents-and-carers provides advice, information about parental controls, developing a family agreement and information on how to discuss online safety with your child.

3. Contact Details

3.1 For any technical questions about your device contact The Olympus Academy Trust IT Department at Olympus IT Helpdesk – Olympus Helpdesk.

3.2 For any issues about learning and keeping safe online please contact your school. Contact details are as follows:

Abbeywood Community School	info@abbeywoodschool.com
Bradley Stoke Community School	admin@bradleystokecs.org.uk
Patchway Community School	pcs-enquiries@olympustrust.co.uk
Winterbourne Academy	office@winterbourneacademy.org.uk
Callicroft Primary School	enquiries@callicroftprimary.org.uk
Charborough Road Primary School	office@charboroughroadprimary.org.uk
Filton Hill Primary School	enquiries@filtonhillprimary.co.uk
Meadowbrook Primary School	office@meadowbrookprimary.co.uk
Stoke Lodge Primary School	slp-enquiries@olympustrust.co.uk

CHILD / YOUNG PERSONS ACCEPTABLE USE AGREEMENT

Rules for using the loaned digital device/laptop and keeping safe online

1. **Agreement**

1.1 I agree to ensure I use the loaned digital device/laptop appropriately for my learning and education. I agree to follow the rules within this Acceptable Use Agreement at all times.

2. **Keeping Safe**

- I will choose my usernames and passwords carefully to protect my identity and I will not share them.
- I will not ask computers to remember my password.
- I must keep my personal details and those of others private.
- I will not visit unsafe sites or register for things I am not old enough for.
- I will log off sites when I have finished.
- I will speak to my parent/carer if I am concerned about any content/messages I see and report them immediately.

3. **Communicating**

- I know that this device is to be used for communication about my learning.
- I know that I need to be polite and friendly online.
- I know that others may have different opinions and that I should respect them.
- I am careful about what I send, as messages can be forwarded on to my parents or head teacher.
- I know that I must have permission to communicate online and will make sure my teacher / parents/carers know who I communicate with.
- I will tell a responsible adult if an online friend wants to meet me and never arrange to meet anyone without permission.
- I will not open messages if the subject field is not polite or if I do not know who it is from, and report it to a responsible adult.

4. **Research and Fun**

- I will use clear search words so that I find the right information and keep safe.
- I know that some content may not be filtered out.
- I know that not everything I find online is factual and will double check information I find online.
- I will use the loaned device for learning and educational purposes only.
- I will not download or stream films/movies/TV programmes, games or other non-educational content.

5. **Sharing**

- I will not use anyone else's work or files without permission.
- Where work is protected by copyright, I will not try to download copies.
- I will not take or share pictures of anyone without their permission.
- I know that anything I put up on the internet can be read by anyone.

6. **Buying and Selling**

- I can tell if a site is trying to sell something.
- I know that I must not buy anything online using this loaned digital device/laptop.

7. **Problems**

- I will not try to change computer settings or install programmes onto this digital device/laptop.
- I will tell my parent/carer if I find anything on a computer that is unpleasant or makes me feel uncomfortable.
- I will not damage the equipment. I will tell my parent/carer if equipment is broken or not working.
- I will not leave this digital device/laptop anywhere outside my home or school.

I agree to use IT by these rules when I use this device whether in school or at home.

My name is .....

Signed ..... Date .....

DOs and DON'Ts

DO take care with information that you share to ensure that it does not compromise the reputation of the Trust or inadvertently convey something confidential or sensitive.

DO report anything you suspect to be a virus to the IT Helpdesk immediately: Olympus Helpdesk.

DO NOT disclose your password to anyone. Literally no-one!

DO NOT leave your laptop anywhere outside your home – especially in a car.

DO NOT open e-mails from unknown people or from people you know which appear suspicious, eg an unexpected subject, unusual content or no appropriate signature block.

DO NOT open e-mail attachments that are unexpected or that look in any way suspicious.

DO NOT visit internet sites that you do not trust or that may contain objectionable material.

DO NOT post inappropriate or offensive remarks, proposals or materials on the internet (e.g. in online forums or on social media such as Facebook or Twitter).

DO NOT use the internet and/or cloud services for anything other than your learning and education.

DO NOT register your school email address for personal use, this includes social media sites such as Facebook/Twitter, banking (e.g. Barclays) or shopping (e.g. Amazon, Tesco).