Information Communication Technology (ICT) Acceptable Use Policy

Version and issue date	1.1 Issued on 21st July 2019
Approved	Board of Trustees 18 July 2019
Scheduled review date	July 2020
Olympus or School policy	Olympus
Statutory or Optional	Non-Statutory
Access	Published on https://www.olympustrust.co.uk/Olympus-Policies-non-statutory/
Appendices	Appendix A ICT Access Denial Form (P.5) Appendix B Social Networking (P.6) Appendix B (i) Relevant legislation (P.10) Appendix C Filtering Policy (P.13) Appendix D E-mail Guidelines for Staff (P.15) Appendix E Advice for the use of Mobile Phones (P.17) Appendix F Rules and Sanctions for one to one devices (P.18)

1) Purpose of the Policy:

The purpose of this policy is to lay down clear expectations for the safe and purposeful use of the ICT resources belonging to, or leased by, the Olympus Academy Trust ('Olympus'' or 'Trust'). It aims to highlight good practice that engages learners, facilitates and enriches teaching and learning and upholds the Trust's duty to safeguard its users of ICT, including compliance with relevant laws. It also recognises the role that parents and carers play in using ICT at home and can be used to support online learning or leisure activities in a supportive manner outside the school context.

The Trust recognises the potential that ICT has to shape the learning and lives of learners in its care. It remains committed to providing an effective and sustainable ICT infrastructure (network, hardware, software and peripherals), fit for supporting teaching and learning in the 21st Century. New technologies form an essential part of young people's lives, both in school and at home. We believe it is our duty to prepare learners for life in the 21st Century through educating them about the safe and effective use of such technologies and providing opportunities for them to explore the digital world and develop their digital literacy in a safe environment.

In all Olympus schools, ICT should be used in a productive and engaging way, not as a teaching tool for its own sake but as a means to an end. It should always be employed purposefully and with definable outcomes focused around a learning agenda. E-safety will always be paramount in our practice, both as one-off events and as planned units in the curriculum at various points. This policy is a key document in ensuring that we deliver the schools' vision for educational excellence as laid out in School Development Plans and via the Olympus School Improvement Strategy.

This policy also lays out expectations for users when using ICT outside the school environment particularly when using school equipment (i.e. a staff laptop). Of particular note for staff is the appendix on social networking (appendix B). All users are expected to act responsibly and to show consideration to others.

This policy also applies to non-teaching staff and those involved with governance (Trust members, trustees and governors).

2) Consultation process:

2.1 This policy was developed in consultation with staff, parents, learners and governors.

3) Relationship to other policies:

Curriculum Policy
Anti-Bullying Policy
Child Protection/Safeguarding Policy
Data Protection Policy
Discipline/Behaviour Policy

4) Roles and Responsibilities:

4.1 **USE OF TECHNOLOGY**

Technology that can be used to store, transmit or manipulate data, such as smart phones, MP3 players, tablets and USB media, should be used responsibly and in accordance with the ICT Acceptable Use Policy, even when not used with school equipment.

4.2 **ACCOUNT SECURITY**

- Users are responsible for the protection of their own network account and must, therefore, keep passwords confidential
- Passwords should be complex; a minimum of 8 characters, which should include upper case and lower case letters, numbers and punctuation marks
- Users may only log on to their own account and must log off when leaving a workstation, even for just a short period of time.
- Log-in details must never be shared for any reason.

4.3 **USE OF FACILITIES**

For all users of ICT it is not acceptable to:

- Attempt to download, store or install software to school computers
- Attempt to introduce a virus or malicious code to the network
- Attempt to bypass network or system security
- Attempt to access another user's account
- Attempt to gain access to an unauthorised area or system
- Attempt to use any form of hacking/cracking software or system
- Connect any device to the network that acts as a Wireless Access Point (WAP), bridge or router
- Connect any device to the network that has access to the Internet via a connection not provided by the school
- Physically damage or vandalise any computer equipment
- Access, download, create, store or transmit material that; is indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful, brings the name of the school in to disrepute (e.g. using the internet in school to download files, materials or applications that could be considered offensive)
- Engage in activities that waste technical support time and resources.

4.4 **PRIVACY AND ESAFETY**

- Users should note that Olympus has a right to access personal areas on the network as they see fit.
- Learners are expected to act safely by not publishing online personal information. They may share interests, ideas, and preferences. Learners must not give out their family name, password, username, e-mail address, home address, school name, city, county or other information that could help someone contact or locate them in person
- It is not acceptable to engage in any behaviour that is upsetting or threatening to another user. Even friendly or flattering comments may be construed as upsetting if they are unsolicited or unwanted. Any form of online bullying will be dealt with in line with the school's Anti-Bullying Policy
- Users should not forward private data without permission from the author.

4.5 **INTERNET ACCESS**

The internet service commissioned via Olympus, including the guest wireless network, is filtered to prevent access to inappropriate content and to maintain the integrity of the computer systems. For more detail on filtering see the Filtering Policy (Appendix C). Users should be aware that Olympus logs all Internet use.

- The use of public chat facilities is not permitted unless directed by a member of staff as part of online learning
- Users should not attempt to use proxy servers to bypass the internet filter system
- Users should not copy and use material from the Internet to gain unfair advantage in their studies, for example in coursework. Such actions may lead to disqualification by examination boards. Information sources must be referenced.
- Users should ensure that they are not breaking copyright restrictions when copying and using material from the Internet.
- Users should not attempt to access or create material that is unlawful, obscene or abusive.

4.6 **E-MAIL**

Automated software scans all e-mail and removes content that could compromise the integrity of the computer systems or contain unsuitable/offensive content.

- Learners are not allowed to use e-mail during lessons, unless the teacher for that lesson has permitted its use
- If a user receives an e-mail from an unknown person or that is offensive or upsetting, an appropriate member of staff should be contacted and reported to the ICT Helpdesk immediately
- They should not delete the e-mail in question until the matter has been investigated
- Sending or forwarding chain e-mails is not acceptable
- Users should not open attachments from senders they do not recognise, or that look suspicious
- Users should periodically delete unwanted sent and received e-mails
- Learners may only use the e-mail facilities provided by Olympus
- Staff and and those involved with governance should always use bcc when using external emails in a group
- Guidance for staff using e-mail is provided in Appendix E.

4.7 **SOCIAL NETWORKING**

Staff, Learners and those involved with governance need to be aware that comments written on any social networking site are public. Any comments written that reflect badly on a school or Trust can result in sanctions. Some social networking (SN) sites are allowed on site if required, usually only as part of a specific job role or activity.

- Learners are not allowed to use SN facilities during lessons, unless the teacher for that lesson has permitted its use
- If a user receives a message from an unknown person, or which is offensive or upsetting, an appropriate staff member should be contacted. Users should perform a

screen shot and paste the message into MS Word, noting the date and time and saving the document until the matter has been investigated

- Only communicate with people on your contact or 'friend' list and be aware that they may be friends with other members of the Trust community who will read the comments you post
- Regularly check your privacy settings to make sure you're only sharing images with friends
- Do not upload images of yourself or others that could be considered inappropriate or damaging
- Do not write or forward messages about others that could be misunderstood or misinterpreted.

4.9 **BLOGS and WIKIS**

The use of blogs and wikis is allowed.

- Learners must agree not to share their user name or password. Learners agree never to log in as another student
- Language that is not appropriate for class is not appropriate for your blog
- Users are expected to conduct themselves as representatives and ambassadors of the school. They must not post comments that are defamatory about the school/Trust, staff or learners or messages which may cause offence or be upsetting
- If a user receives a message from an unknown person, or which is offensive or upsetting, an appropriate staff member should be contacted
- Users must respect other users' work and opinions and not maliciously edit any group or individual work. Any user who feels this has taken place should leave the work as it is and contact a relevant member staff.

4.10 **VIRTUAL LEARNING ENVIRONMENT**

Individual schools may offer their own virtual learning environment for use by learners and parents/carers. There may be a separate acceptable use policy in regard to this, which will be administered by the school itself.

4.11 **PRIVATELY OWNED COMPUTERS**

Personal laptops and desktops are allowed to be brought into Trust premises to be used for teaching and learning or other appropriate purposes (eg. Governance). The Trust will not be responsible for any damage or theft of these devices and as a result recommends staff and learners seek out their own device insurance. Please see Appendix F for rules and sanctions for one-to-one device use.

It is assumed that parents/carers grant their child the right to access the network unless a permission denial form is signed and returned (Appendix A)**.**

Please be aware that ICT is used throughout the schools in all subjects. Without access to the network, your child will not be able to access some aspects of the curriculum. You may opt to deny access to e-mail or the internet, which will have a smaller impact on your child's ability to access the curriculum than denial of all network access.

5) Monitoring and review:

The Trust will review this policy in a yearly cycle, to assess its implementation and effectiveness.

Appendix A - ICT Access denial form

Dear parents/carers

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

Please be aware that ICT 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 ICT network, please return this form to reception for the attention of ICT support:

Name of Student_____

Year_____ **Tutor group**_____

As the parent or legal guardian of the student 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 B - Social Networking Policy

1) Purpose

1.1 Objectives

This policy sets out Olympus Academy Trust's policy on social networking and aims to:

- Assist the Trust's staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice
- Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Support safer working practice
- Minimise the risk of misplaced or malicious allegations made against adults who work with learners
- Prevent adults abusing or misusing their position of trust.

1.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in school will always advise the Headteacher of the justification for any such action already taken or proposed. The Headteacher will in turn seek advice from the Trust's CEO or Executive Headteacher and Trust Board where appropriate.

1.1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations the Trust Board and the relevant legislation listed below.

1.2 Scope

1.2.1 This document applies to all adults who work for The Olympus Academy Trust as adopted by the Trust Board. This includes teachers, support staff, supply staff, governors, trustees and volunteers.

1.2.2 It should be followed by any adult whose work brings them into contact with learners. References to adults should be taken to apply to all the above groups of people in school. Reference to learners means all learners at the school including those over the age of 18.

1.2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them

1.3 Status

1.3.1 This document does not replace or take priority over advice given in other policies or the Trust's codes of conduct when dealing with allegations of abuse or other policies issued around safeguarding or ICT issues, but is intended to both supplement and complement any such documents.

Principles

- Adults who work with learners are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions
- Adults in school should work and be seen to work, in an open and transparent way.

- Adults in school should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

2) Safer Social Media Practice

2.1 **What is social media?**

2.1.1 For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook are perhaps the most well-known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day

2.1.2 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

4.2 Overview and expectations

4.2.1 All adults working with learners have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of learners. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, learners, public in general and all those with whom they work in line with the Trust's code of conduct. Adults in contact with learners should, therefore, understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.

4.2.2 The guidance contained in this policy is an attempt to identify what behaviours are expected of adults within the school setting who work with or have contact with learners. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and may result in disciplinary action being taken against them

4.2.3 Adults within the school setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They should report and record any incident with this potential.

4.3 Safer online behaviour

4.3.1 Managing personal information effectively makes it far less likely that information will be misused

4.3.2 In their own interests, adults within school settings need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for learners or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties

4.3.3 All adults, particularly those new to the school setting, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site

4.3.4 Adults should never make a 'friend' of a student at the school where they are working on their social networking page, and should be cautious about becoming 'friends' with ex-learners where siblings continue to attend the school

4.3.5 Staff should never use or access social networking pages of learners and should never accept an invitation or invite a student to become a 'friend'

4.3.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put

any confidential information or images on their site about themselves, their employer, their colleagues, learners or members of the public

4.3.7 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, learners or other individuals connected with the school, could result in formal action being taken against them

4.3.8 Adults are also reminded that they must comply with the requirements of equalities legislation in their online communications

4.3.9 Adults within the school setting must never post derogatory remarks or offensive comments online or engage in online activities which may bring the school into disrepute or could reflect negatively on their professionalism.

4.3.10 Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher/teaching assistant, you should not put any information onto the site that could identify either your profession or the school where you work. Staff are strongly advised to remove their place of work from social media sites to avoid potential conflict. In some circumstances this could damage the reputation of the school, the profession or the Trust.

4.4 Protection of personal information

Adults working in school should:

4.4.1 Never share their work log-ins or passwords with other people, or allow others to observe the entry of your password

4.4.2 Lock the computer with a password (unless the user is prepared to log off) every time they leave a computer that they are using

4.4.3 Ensure that that computer is not left unattended when logged in.

4.4.4 Keep their personal phone numbers private

4.4.5 Not give their personal e-mail addresses to learners or parents. Where there is a need for homework to be sent electronically, the school e-mail address should be used

4.4.6 Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises

4.4.7 Understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people

4.4.8 Adults working in school should ***not*** use their own mobile phones to contact learners or parents.

4.5 Communication between learners / adults working in school

4.5.1 Communication between learners and adults by whatever method, should take place within clear and explicit professional boundaries

4.5.2 This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs

4.5.3 The school normally provides a work mobile and e-mail address for communication between staff and learners where this is necessary for particular trips/assignments. Adults should not give their personal mobile numbers or personal e-mail addresses to learners or parents for these purposes

4.5.4 Adults should not request, or respond to, any personal information from a student, other than that which might be appropriate as part of their professional role

4.5.5 Adults should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with learners so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending

4.5.6 Adults should not give their personal contact details to learners including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with a member of the school's leadership team and parents/carers

4.5.7 E-mail or text communications between an adult and a student outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications

through internet based websites. Internal e-mail systems should only be used in accordance with the Trust's policy.

4.5.8 Trust equipment must NOT be used for:

- Personal use, unless it has been authorised by the Business Manager and appropriate insurance has been obtained (e.g. camera or recording equipment)
- Any illegal purpose
- Engaging in online gambling
- Distributing copyrighted information in breach of copyright
- Setting up internet sites
- Anything else which it is not appropriate to access or use it for, either in the view of the relevant chair (for trustees, governors or committee members) or the CEO (for other users) or in the view of the user themselves.

4.6 Social contact

4.6.1 Adults should not establish or seek to establish social contact via social media / other communication technologies with learners

4.6.2 There will be occasions when there are social contacts between learners and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged with the Associate Headteacher or Headteacher where there may be implications for the adult and their position within the school setting

4.6.3 There must be awareness on the part of those working with or in contact with learners that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the adult's own family.

4.7 Access to inappropriate images and internet usage

4.7.1 There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and disciplinary action being taken

4.7.2 Adults should not use equipment belonging to their school/Trust to access any pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children

4.7.3 Adults should ensure that learners are not exposed to any inappropriate images or web links

4.7.4 Where indecent images of children are found, the police, local authority designated officer (LADO) and school Child Protection Officer should be immediately informed. Colleagues should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution

4.7.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, either the Headteacher or the LADO should be informed and advice sought. The CEO or Executive Headteacher should be informed. Colleagues should not attempt to investigate or evaluate the material themselves until such advice is received.

4.8 Cyber-bullying

4.8.1 Cyber-bullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'

4.8.2 Prevention activities are key to ensuring that adults are protected from the potential threat of cyber-bullying. All adults are reminded of the need to protect themselves from the potential threat of cyber-bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.

4.8.3 If cyber-bullying does take place, staff should keep records of the abuse, text, emails, website or instant message and should not delete texts or e-mails. Employees are advised to

take screen prints of messages or web pages and be careful to record the time, date and place of the site

4.8.4 Adults may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process

4.8.5 Adults are encouraged to report all incidents of cyber-bullying to their line manager or the Associate Headteacher or Headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police

4.8.6 Adults should be familiar with the Cyber-Bullying Policy and know what to do in the event that a child discloses that they are being cyber-bullied.

5) Review

5.1.1 Due to the ever changing nature of information and communication technologies it is best practice that this policy be reviewed bi-annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

6) Appendix B (i)

All users should be aware of the legislative framework which surrounds use of social media / communication technology in the UK. In general terms, an action that is illegal if committed offline is also illegal if committed online.

General Data Protection Regulations (GDPR)

GDPR is a regulation in EU law, adopted by the UK, on data protection and privacy for all individuals within the European Union (EU). It sets guidelines for the collection and processing of personal information of individuals.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer or to programs or data;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject’s rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have

obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
    - Ascertain whether the communication is business or personal;
    - Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994
This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study.

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust (typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007. Obscene publications act 1959 and 1964. Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Appendix C – Filtering Policy

Filtering Policy

Introduction

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. It is, therefore, important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the school's context. As a part its broadband provision, Olympus schools and connected organisations automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level. In addition to this, the Olympus Network has its own filtering software that is regularly updated to help increase the protection and flexibility.

Responsibilities

The responsibility for the management of the school's filtering policy will be held by The Strategic lead for ICT and The Technical Director. 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 to change control logs
- be reported to a second responsible person, and the member of staff responsible for whole school ICT, as and when they happen.
- be reported to the Audit and Risk Committee once a year in the form of an audit of the change control log.

All users have a responsibility to immediately report to the ICT Helpdesk (helpdesk@olympustrust.co.uk), any infringements of the school/Trust's filtering or any sites that are accessed, which they believe should have been filtered.

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

Education / Training / Awareness

Learners will be made aware of the importance of filtering systems through the school's e-safety education programme and by being prompted to read and accept the ICT Acceptable Use Policy (AUP) every time that they access ICT systems. They will also be warned of the consequences of attempting to subvert these filtering systems.

Staff users will be made aware of the filtering systems through an automated prompt each time they access ICT systems.

Parents/carers will be informed of the school's filtering policy through the ICT Acceptable Use Policy, the school's website, newsletters and texts.

Changes to the Filtering System

If a member of staff needs a site unblocked, they need to:

- Send a request to the ICT Helpdesk ((helpdesk@olympustrust.co.uk). Include the details of the website to be unblocked (include: web address, reason for unblocking the site and the date it needs to be unlocked by). The request will then be passed to their line manager and the Technical Director who will examine the site for inappropriate content, review any potential security risks and make a reasoned decision about whether access is required to fulfil the responsibilities in their job description.

- The un-filtering of a site should only be requested if the content of the site has educational merit, does not feature sexual, violent or inappropriate content and bears no risk to the stability of the school network.
- Confirmation of the decision will be returned to the requestor and their line manager within 5 school days of the original request.

If learners require access to specific websites subject to Local Authorities filtering, they should approach their teacher who can assess the need from a learning context and complete the relevant form as appropriate.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

- School/Trust ICT Lead
- Student Support Team
- Executive Leadership Team

Appendix D - E-mail Guidelines for Staff

New messages

1. Always complete the subject box so colleagues can be selective about what they read
2. Avoid sending e-mails to all staff unless it is about a student and you don't know who teaches them. Make sure you include the student's initial and Teaching Group in the subject line. E.g. JE 7B = Joe Emery 7B
3. If you are sending an email to a group that include external addresses (i.e. student or parents) always use BCC. Sharing external email addresses without consent is a breach of the Data Protection Act and must be reported to the Trust's Data Protection Officer.
4. Be mindful when mentioning others in e-mails. Under the Data Protection Act, any information we hold about an individual, in any format, must be shared if requested
5. When you send a message to someone that requires an action, make it very clear within the first few lines of the e-mail what is expected. If possible, you should also include a due date
6. Use the options button to indicate if the e-mail is urgent or sensitive – it helps recipients to be selective
7. Try to avoid sending unnecessarily long e-mails – keep it brief and to the point

Signatures

1. Ensure the branded signature is used for all e-mails. This should be the shorter version with just your name and job title for internal communication and the longer one including contact details for external emails.
2. If your e-mail is in connection with the academy chain business (e.g. payroll or personnel), use the official Olympus e-mail signature.

Replying to e-mails

1. Before replying, ask yourself whether all of the people on the recipient list really need to see your reply
2. If you are angry or upset about the message you are replying to, give yourself some time to calm down before replying. Reading through your reply several times will also help. Sending a quick and angry response rarely helps and often leads to an increasingly acrimonious exchange of messages

Forwarding e-mails

1. Follow the same rules as for "replying to e-mails"
2. Consider including a summary at the beginning. This will allow the new recipient to determine what has already been discussed

Attachments

1. Be **selective** in the sending of attachments: wherever possible either include the text in the body of the e-mail
2. Think carefully about their size. Files in text (txt), revisable text format (rtf) and portable document format (pdf) are usually more compact formats than files in Word (doc) format. In addition, they are less prone to carry viruses
3. Be very careful when opening attachments, even if the message appears to be from someone you know. E-mail attachments infected with viruses are one of the most widely used methods for infecting PCs
4. Put large files into a folder on the shared files. E-mail your recipients with the location or provide a link to direct them there rather than attaching the file to your e-mail

Managing e-mail

1. Delete all unwanted messages and messages that have been dealt with – this will make your mailbox easier to manage and will save storage space
2. Your inbox should not be used to store messages you wish to keep; they should be moved into a different folder

3. Ask ICT support if you would like a local archive for emails. This will enable you to save emails you need to keep on your machine and so reduce the size of your mail box.
4. To avoid an over-dependence on e-mails, check them twice a day – don't keep it logged on or you will become distracted by incoming e-mails.

Managing expectations

1. Try not to make a habit of sending e-mails late outside of usual working hours (8am-5pm) It sends the wrong signals to colleagues about your expectations of their response – colleagues need not respond to messages sent outside of this time, or in less than a 24 hour timescale in normal circumstances.
2. Use a phone call, meeting or even a conversation as an alternative to long or potentially sensitive e-mails.
3. Be careful how you express yourself – especially if you feel heated about a subject. Email lacks the social cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.

Appendix E - Advice for the use of Mobile Phones

Rules for *secondary phase* learners

- All phones and MP3 players etc. should be turned off and placed in your locker as soon as you arrive in school
- They should stay in your locker all day and should not be taken into class or used in the corridor
- If you need to contact home urgently you should go to reception to do this and not go to your locker to text home; parents should contact reception if they need to get an urgent message to you
- You may not take any images or videos of learners or members of staff without permission
- You may not text or make a phone call in school
- You must never post images of staff or learners in school on any website, social networking site or similar …. and you should not write about them in an offensive or slanderous manner.

Rules for *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.

Rules for *Post 16* learners

- Post 16 students 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 miss-use of this privilege may result in it being withdrawn.

Rules for *staff*, *governors,* or any *other visitors*

- Staff should not take pictures of any student or store any information relating to students 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.

Consequences

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

Appendix F – One-to-One devices. Rules and sanctions.

(please note this only applies to learners if the school permits use of one-to-one devices in school. There are no additional rules/sanctions for adult users (e.g. staff, governors and other visitors) in addition to sections 1-5 of the main policy.

Rules for device use (students):

- In standard classrooms devices should be shut and on the desk in front of learners. Learners need to check with their teacher at the beginning of the lesson that they are happy for them to use them when appropriate e.g. to take notes, research etc
- Devices can only be used within lessons
- Any devices being used outside of lessons will be confiscated
- Learners are not permitted to take devices into toilets or changing rooms, they must be placed in their lockers. Any student caught with devices in these areas will receive a device ban
- Learners may not upload any information, images, videos or comments about peers or staff without permission
- The devices are meant for learning and any use of the devices that deviates from that will be considered inappropriate use e.g. chatting, games, watching irrelevant videos
- Malicious damage to school/Trust network or devices or other student's devices will be dealt with in line with the Acceptable Use Policy ('AUP') and the school's behaviour policy and the cost of repairs will be charged to the parents
- Learners may not use their device for sending, sharing or displaying obscene or offensive material
- Any tablet, laptop or iPad is fine but no mobile phones (if it can make a phone call it's not suitable)
- Learners need to make sure they understand the AUP and behaviour policies, by bringing a device in they agree to abide by them
- Learners will not be permitted to charge their devices in schools, they need to come prepared!

Sanctions for inappropriate use*

*Inappropriate use will be based on the teacher's judgement and is loosely defined to include, but not restricted to, use of a device when not allowed or breach of any of the device rules outlined above

Within class

- Learners will receive a warning
- Continued misuse will result in learners being told to shut the device and place it on the desk.
- Any further inappropriate use will result in the teacher confiscating the device

- Learners may receive a device ban for a prolonged period if they demonstrate they can't be trusted to behave responsibly

- Serious breach of device rules for use can result in exclusion or loss of access to IT in school

Outside of lessons

- Any student caught using their device outside of lessons will have the device confiscated.

Device confiscation

- If a device is confiscated the member of staff will store it in a sealed bag with the student's name on. The device will then be taken to Student Services at the first opportunity. The student can collect their device at the end of the day

- If learners have had their device confiscated twice in any term their parents will need to come in and reclaim the device. A member of Leadership Team will then meet with the student and their parents to discuss how to behave responsibly

- Three or more device confiscations will result in a device ban for a period of time, determined on a case by case basis, but no less than a term.

- If learners refuse to hand over device – this will result in isolation and device ban. We will also meet with parents to discuss whether learners can have a device in lesson.

Serious misuse of ICT

Any serious breach of the rules including (but not restricted to) cyberbullying, taking or uploading images or videos of staff or learners without permission, use of a device in toilet or changing rooms will result in the following:

- The student going straight to Student Support Team who will investigate
- LT detention
- Device ban
- If it is determined that it is a serious misuse of ICT then a fixed term exclusion

Any student causing damage or behaviour problems in or out of class through interfering with some-else's device can expect normal behaviour sanctions. Any damage caused the student responsible will be asked to pay for it.