Westfield Academy
Seeing the qualities in every child

# ICT Acceptable Usage / E Safety Policy

**Approval Date – May 2014** **Review Date – May 2017**

It is the policy of the governors of Westfield Academy that students should be encouraged to fully utilise the potential of technology to enhance their learning and that they should be taught to be discerning, effective, responsible and safe users of ICT. The policy is informed by the SWGFL (South West Grid for Learning) Policy Guidelines. This policy applies to all users.

## Rationale

New technologies are integral to the lives of most people, especially the young. Used properly they can help promote and enhance learning. Young people should be able to use these technologies safely and appropriately

**This Policy is intended to ensure:**

- That young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

In all areas of the curriculum where mobile technologies and information-based technologies are used, students will be taught:

- About the importance of e-safety and how to keep themselves safe.
- How to recognise issues of risk, safety and responsibility surrounding the use of ICT.
- How to access help, for example from the student e-safety desktop icon.
- The importance of abiding by the acceptable useage procedure.

## Roles and Responsibilities

### 1.1 Governors

Governors are responsible for the approval of the ICT Acceptable Usage / E Safety Policy policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors student Matters Sub Committee. A member of the Governing Body has taken on the role of ICT / E-Safety Governor. The role will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to relevant Governors committee / meeting

### 1.2 The Principal

The Principal has overall responsibility for the progress and welfare of students including their use of ICT to facilitate safe and effective learning. This responsibility is delegated in part to the ICT Department, ICT Manager and Assistant Principal (Inclusion) for issues relating to specific usage and the strategic direction of ICT and the E-Safety coordinator for day to day responsibility for E- Safety

- The Principal / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Principal / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator
- **The Principal and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see Appendix; SWGfL flow chart on dealing with e-safety incidents –"Responding to incidents of misuse" and relevant Local Authority HR / disciplinary procedures)

### 1.3 E-Safety Coordinator (IT Manager)

- Leads the e-safety committee
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and regularly updated advice for staff
- Liaises with the Local Authority
- Liaises with school ICT technical staff
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments, (Examples of suitable log sheets may be found in the SWGfL Safety and Security Booklet, along with the Internet Safety Protocol)
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs
- Attends relevant meetings / committee of Governors
- Reports regularly to Senior Leadership Team

### 1.4 The Designated Person for Child Protection (Assistant Principal Inclusion)

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

**1.5 The IT Manager / Technical Staff** are responsible for ensuring:

- **That the school's ICT infrastructure is secure and is not open to misuse or malicious attack**
- That the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- SWGfL is informed of issues relating to the filtering applied by the Grid
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

**1.6 Lead Teacher for ICT**

Will oversee the provision of E-Safety Education to students. E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

**1.7 Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the E-Safety Co-ordinator / IT Manager as appropriate
- Digital communications with students should be on a professional level and only carried out using official school systems
- Students / pupils understand and follow the school e-safety and acceptable use policy
- Students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities using Impero monitoring software where appropriate
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

**1.8 Students**

Students must:

- Obtain the permission of parent(s)/guardian(s) before they are allowed to use the Internet. A consent form must be signed and returned to the school.
- Never reveal personal information, either their own or others, such as home addresses, telephone numbers and personal Email addresses.
- Keep their log on details and password secret.
- Only access those services that they have been given permission to use.
- Never use photographs of themselves on the Web unless the parent or guardian has given permission to do so.
- Never meet people in person that they have contacted on the Internet without parent/guardian permission.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Be aware that the author of an email or web page may not be the person they claim to be.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Never download, load or install any software, shareware, or freeware onto their school network user area
- Not copy other people's work or intrude into other people's files without permission.
- Never logon to the network using the username and password of another user.

Behaviour Code

Students are responsible for appropriate behaviour on the school's computer network, just as they are in the classroom or on the school playground. Communications on the network are often public in nature. General school rules and our Behaviour Policy apply and users must comply with the guidelines of this policy. Students are personally responsible for their actions when using school equipment to access computer resources outside the school network. These rules apply to both school owned equipment and to any permitted internet enabled mobile devices brought onto site by students.

Students are allowed to bring their own internet enabled devices (Lap tops, game machines, mobile phones etc.) into school but these may only be used at break and lunch times and in lessons with the teacher's permission. At all other times they must not be used and must be kept out of sight.

Where we suspect that a student owned device has been used in an inappropriate manner, the device will be confiscated and its content viewed and possibly deleted, in accordance with the government's 'Screening, Searching and Confiscation' guidance for schools (Education act 2011) and the school's Behaviour Policy.

Inappropriate Materials or Language

Profane, abusive or impolite language must not be used to communicate nor should materials be accessed which are not in line with the rules of school behaviour – a good rule to follow is never view, send, or access materials that you would not want your teachers or parents to see. Should students encounter such material, they should immediately report it to their teacher.` No non-educational Internet games may be played during school hours.

Users must never use the computers to engage in activities that may be in violation of the law.

### 1.9 Parents

Parents must:

- Give permission for their child to use the school's computer network and the Internet. A consent form must be signed and returned to the school.
- Be aware of the school's policy for access to the Internet and use of the school computer network.
- Recognise the fact that the school uses a filtered Internet service and have introduced procedures that should enable students to use the Internet facilities safely and securely.
- Take full responsibility for how students use the Internet outside school.

### 2.0 Community Users

All Community Users must adhere to this policy and in particular to its purpose and principles as stated above. Community Users must never use the computers to engage in activities that may be in violation of the law.

### Related Documents

Appendix 1 – Acceptable Usage Agreement
Appendix 2 – Guidance for Staff

### Monitoring

This policy is monitored by the Governors' Student Matters Sub-Committee by using the following evidence:

- A report from the IT manager and teacher responsible for ICT.
- A member of the sub-committee interviewing staff about their usage of ICT.

### Responsible

- Chris Hunt (Principal)

Appendix 1 – Acceptable Usage Agreement

## ICT ACCEPTABLE USAGE AGREEMENT

### 1. INTRODUCTION

Westfield Community School will allow students, teachers, other employees and the community access to its computers, network services, and the Internet.

All activity, when using the network and Internet in school, must be in support of education and/or research and must be appropriate to the educational objectives of the School. All Internet activity is logged. Students, staff and other members of the community who access the Internet from the school site are responsible for everything that takes place *under their login* (on their computers).

*Students are permitted to bring in their own mobile devices to use on our wireless network. However they do so at their own risk and the school cannot accept any responsibility for loss or damage however caused. Use of these devices must only be with the permission of staff in lessons, or in designated areas at break and lunchtime.*

### 2. PURPOSE

Access to ICT and the Internet will enable users to:

- Explore thousands of libraries, databases, museums, and other repositories of information.
- Exchange personal communication with other Internet users around the world.
- Be included in Government initiatives and global educational projects.
- Keep abreast of news and current events.
- Take part in live discussion with experts.
- Publish and display work by creating personal Web pages.
- Use a range of tools to enhance their work.

### 3. PRINCIPLES

Use of ICT and Internet access will be planned to enrich and extend learning activities as an integral aspect of the curriculum. Students will be given clear objectives of Internet use *and* be educated in responsible and effective Internet use. They will be supervised appropriately and learn to search for and discriminate between valid and inappropriate material and to learn to copy, save and use material found on the Internet without infringing copyright.

### 4. SAFETY

Internet access both through the site network and wireless system at Westfield is filtered by The Somerset County Internet Service Provider and our own safety software but ultimately, staff, parents, students and other users are responsible for setting and conveying the standards that should be followed when using media and information sources. Students using their own devices (notebooks/laptops/mobile phones etc) to access the school's Wireless network must enter the correct settings and password which will then allow them filtered access to the internet.

All School Network Web activity is logged so that activity by all users can be monitored. Access to our public filtered wi-fi via students own devices is not logged.

**Student Agreement**

I have read, understood and accept the ICT Acceptable Usage Policy, including appendix 1.

Pupil Name: _____ Tutor group: _____

Signature of Student: _____ Date: _____

This form must be completed, signed and returned to your Form Tutor for central records.

**Parental Agreement**

As a parent/guardian I have read the above policy for access to the Internet and use of the school computer network. I recognise the fact that although the school uses a filtered Internet service, the school staff may have difficulty restricting access to all the controversial materials on the Internet. Therefore I will not hold them responsible for materials that my child may find as a result of using the Internet through school facilities. I take full responsibility for how my child uses the Internet outside school.

Signature of parent/guardian: _____ Date: _____

Print name: _____

**Staff Agreement**

I have read, understood and accept the ICT Acceptable Usage Policy, including all appendix 1 and 2.

Name of Staff Member: _____

Signature of Staff Member: _____

Date: _____

Appendix 2 - Guidance for Staff

**E-Safety Guidance for Staff**

**Rationale**

All staff must ensure that students are responsible and safe users of ICT. They should also ensure that they only use school technologies to support them in carrying out their professional role appropriately. Staff must not run the risk of making themselves personally vulnerable by using technologies to communicate inappropriately with students.

**All staff must:**

- Adhere to ICT acceptable users' policy and in particular to its purpose and principles.
- Use the school ICT network for carrying out their job appropriately.
- Supervise students using ICT appropriately to ensure this policy is implemented.
- Ensure that students are using the system responsibly and that this policy is being adhered to using Impero monitoring software where appropriate.
- Not use the school network for private purposes during normal school hours, or for trading with other users of the network for private gain.
- Be aware that the school network is not private, and that network managers can and do look at data.
- Never use ICT to engage in activities that may be in violation of the law.
- Have an up to date awareness of e-safety matters and of the current school e-safety and Data Protection policy and practices
- Not have present or past students as "friends" on social networking sites (for these purposes, past is defined as within the past 5 years).
- Not have contact details of students on their own personal devices.
- Report any break of this code, suspected misuse or problem to the E-Safety Co-ordinator / IT Manager as appropriate
- Have a strong password and ensure other users do not have access to it.
- Ensure computers are always locked when not in use.
- When working remotely using school data, ensure that all appropriate e-safety measures are taken.
- Be aware of the latest legislation regarding the movement of Student Data off the school network. All data moved (eg by usb stick, transfer to hard disk, laptop, tablet, mobile phone etc) must be encrypted. This includes any data transferred from remote access to a local (home) computer.

Staff should note the section on ICT from the Staff Code of Conduct (Staff Handbook):

**"ICT** – Staff must use ICT for carrying out their job appropriately. It must not be used for private purposes including social networking during normal school hours or for trading with other network users. Staff must ensure privacy and data protection by ensuring their log-on password is confidential and must lock their computer when not in use. Staff must not use personal devices during the school day, must not keep personal contact details of students, ex-students or parents on personal devices and must not have any of these groups as "friends" when using social networking media. Staff must take reasonable steps to protect their professional integrity."

Inappropriate use will be subject to the Staff Disciplinary code.