Iffley Academy
e-Safety Policy

Written	December 2019
Date of review	December 2021
SLT Lead	S Wawrzyniak
Signed: Head Teacher	_____
Chair of Trustees	_____

Aim

To ensure that students and staff of the Iffley Academy stay safe online, whilst using digital media and are fully equipped with the protective behaviours to resist peer pressure, radicalisation, cyber-bullying, online exploitation and are confident to report issues as and when they arise. It is therefore essential that everyone involved with the academy takes responsibility for promoting a positive safe culture online, models appropriate behaviour and challenges inappropriate conduct.

Teaching and learning

The rapid developments in electronic communications are having a major impact on society. The Iffley Academy needs to ensure that it equips its pupils with the ability to use electronic communications in a safe, secure, productive and efficient way.

Safe use of the Internet is part of the statutory curriculum and a necessary tool for learning. It is a part of everyday life for education, business and social interaction. Understanding of social media and development of sites such as blogs has been included in the new curriculum and it is essential that this can be implemented in a safe and successful way. The school has a duty to provide students with quality Internet access as part of their learning experience.

The school recognises that pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security. The school also recognises that we have a growing cohort of vulnerable complex need students who will be more vulnerable on the Internet.

The aim of e-communications is to have a positive impact on learning outcomes. Developing effective practice in using the Internet for teaching and learning is essential.

Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

Key Principles for internet use:

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The Academy can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- All users will be expected to behave in a safe and responsible way, promote a respectful culture online and ensure that technology is being used to aid learning.
- The use of mobile phones in school as set out in the BYOD policy will be explained to new staff and new students.

Managing Information Systems

The ICT Technician will continually review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

The Technician and other staff will adhere to Oxfordshire County Council policy “ICT Acceptable Use Policy”. The Technician and other staff will adhere to The Iffley Academy policy “The BYOD Policy”.

Key principles:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use. Flouting the electronic use policy is regarded as a disciplinary matter.
- Workstations should be secured against user mistakes and deliberate actions.

- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed.
- All Internet connections must be arranged to ensure compliance with the security policy.
- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT technician will review system capacity regularly.

Use of email

- Email is an essential means of communication for both staff and pupils, although appropriate safety measures must be put in place.
- Email should not be considered private and the school reserves the right to monitor email.
- Email accounts will not be provided which can be used to identify both a student's full name and the school.

Key Principles:

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff should not use personal email accounts during school hours or for professional purposes

Website management

As the school's website is openly available, publication of information must be considered from a personal and school security viewpoint. Our previous policy stated that *"It is not appropriate to place material such as staff lists or a school plan on the public website."* Whilst staff safety is paramount the school also understands the needs of the growing ASC cohort and that staff lists and photos of

staff being available on the website can be incredibly helpful. For this reason staff photos and names are posted on the website unless staff wish to opt out. Staff will be informed when photographs are taken that their intended use is on the website and that they have the right to opt out.

Key Principles:

- The security of staff and pupils is paramount.
- Images of a pupil should not be published without the parent's or carer's permission.

Social networking, social media

Key Principles:

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out/make public personal details of any kind which may identify them and / or their location. Examples would include full real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Where appropriate information regarding 'location settings' will be taught to students so that they are not giving out their location and potentially their home address to others online.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- The school will work with external ICT teams to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the Trust Learning Manager for ICT.
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.

How is the Internet used across the community?

Key Principles:

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- Clear procedures are in place to support anyone affected by Cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
    - Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
    - The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Outcomes for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - Social media sites and/or service providers may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers may be informed.
    - The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms and learning environments be managed?

Key Principles:

- SLT and staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.

- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways.
    - The user will be asked to remove any material deemed to be inappropriate or offensive.
    - The material will be removed by the site administrator if the user does not comply.
    - Access to the LP for the user may be suspended.
    - The user will need to discuss the issues with a member of SLT before reinstatement. A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff.

Communications Policy

Key Principles:

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Pupil instruction in responsible and safe use should precede Internet access.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

School blog

The Iffley Academy during the time as Iffley School, has used online blogs for students to develop their learning. The Iffley Academy may continue to do this in the future and will abide by the following key principles.

- The blog will be managed by the school and all content will be moderated.
- Anonymous comments will be disabled.

- Explicit or inappropriate comments will not be allowed and will be followed up. This may be in house or could involve contacting external bodies such as service providers and/or the police.
- Safe use of blogging will be taught in lesson times before students are encouraged to post.
- Students images will only be used with the permission of parents/carers and safeguarding and child protection issues will be considered as a priority at all times.
- Inexperienced members of staff will not be given administrator access without clear guidance.
- A member of SLT will have the authority to remove content and other administrators if they feel necessary.

Appendix 1 - Cyber-bullying
Key Safety Advice For Children & Young People

1. Always respect others – be careful what you say online and what images you send.

2. Think before you send – whatever you send can be made public very quickly and could stay online forever.

3. Treat your password like your toothbrush – keep it to yourself. Only give your mobile number or personal website address to trusted friends.

4. Block the bully – learn how to block or report someone who is behaving badly.

5. Don't retaliate or reply!

6. Save the evidence – learn how to keep records of offending messages, pictures or online conversations.

7. Make sure you tell:
   - an adult you trust, or call a helpline like ChildLine on 0800 1111 in confidence;
   - the provider of the service;
   - check the service provider's website to see where to report incidents;
   - your school – your form tutor or another adult at school can help you.

Finally, don't just stand there – if you see cyber-bullying going on, support the victim and report the bullying. How would you feel if no one stood up for you?

Key Safety Advice For Parents & Carers

1. Be aware, your child may as likely cyberbully as be a target of cyber-bullying. Be alert to your child seeming upset after using the internet or their mobile. This might involve subtle comments or changes in relationships with friends. They might be unwilling to talk or be secretive about their online activities and mobile phone use.

2. Talk with your children and understand the ways in which they are using the Internet and their mobile phone.

3. Use the tools on the service and turn on in-built internet safety features.

4. Remind your child not to retaliate.

5. Keep the evidence of offending emails, text messages or online conversations.

6. Report cyber-bullying:
   - Contact your child's school if it involves another student, so that they can take appropriate action.
   - Contact the service provider.
   - If the cyber-bullying causes alarm or distress eg. being threatened, this is a criminal offence, you should consider contacting the police.

The table below explores the range of ways today's technology can be used.

Great for	Examples of misuse
Mobile phone Keeping in touch by voice or text, taking and sending pictures and film, listening to music, playing games, going online and sending emails. Useful in emergency situations and for allowing children a greater sense of independence.	**Mobile phone** Sending nasty calls or text messages, including threats, intimidation, and harassment. Taking and sharing humiliating and/or inappropriate images. Videoing other people being harassed and sending these to other phones or internet sites.
Instant messenger (IM) or equivalent Text or voice chatting live with friends online. A quick and effective way of keeping in touch even while working on other things.	**Instant messenger (IM) or equivalent** Sending nasty messages or content. Using someone else's account to forward rude or mean messages via their contacts list.
Chatrooms & message boards Groups of people around the world can text or voice chat live about common interests.	**Chatrooms & message boards** Sending nasty or threatening anonymous messages. Groups of people deciding to

For young people, this can be an easy way to explore issues which they are too shy to talk about in person.	pick on or ignore individuals. Making friends under false pretences – people pretending to be someone they're not in order to get personal information that they can misuse in a range of ways – e.g. by spreading secrets or blackmailing.
Emails Sending electronic letters, pictures and other files quickly and cheaply anywhere in the world.	**Emails** Sending nasty or threatening messages. Forwarding unsuitable content including images and video clips, or sending computer viruses. Accessing someone else's account, e.g. to forward personal emails or delete emails.
Webcams Taking pictures or recording messages. Being able to see and talk to someone live on your computer screen. Bringing far-off places to life or video conferencing.	**Webcams** Making and sending inappropriate content. Persuading or threatening young people to act in inappropriate ways. Using inappropriate recordings to manipulate young people.
Social network Sites Socialising with your friends. Allowing young people to be creative online, even publishing online music. Personalising homepages and profiles, creating and uploading content.	**Social network Sites** Posting nasty comments, humiliating images / video. Accessing another person's account details and sending unpleasant messages, deleting information or making private information public. Groups of people picking on individuals by excluding them. Creating fake profiles to pretend to be someone else, e.g. to bully, harass or get the person into trouble.
Video hosting sites Accessing useful educational, entertaining and original creative video content and uploading your own.	**Video hosting sites** Posting embarrassing, humiliating film of someone
Virtual Learning Environment School site, usually available from home and school, set up for tracking and recording student assignments, tests and	**Virtual Learning Environment** Posting inappropriate messages or images. Hacking into someone else's account to post inappropriate comments or delete schoolwork.

activities, with message boards, chat and IM.	
Gaming sites Consoles & Virtual world Live text or voice chat during online gaming between players across the world, or on handheld consoles with people in the same local area. Virtual worlds let users design their own	**Gaming sites Consoles & Virtual world** Name-calling, making abusive / derogatory remarks. Players may pick on weaker or less experienced users, repeatedly killing their characters. Forwarding unwanted messages to avatars – a figure that represents them in the virtual world. other devices in the immediate vicinity.

Mobile phones

All UK mobile phone operators have nuisance call centres set up and / or procedures in place to deal with such instances. They may be able to change the number of the person being bullied. Mobile operators cannot bar a particular number from contacting a phone, but some phone handsets do have this capacity. Action can be taken against the bully's phone account (e.g. blocking their account) only with police involvement.

Social networking sites (e.g.facebook etc.)

It is good practice for social network providers to make reporting incidents of cyber-bullying easy, and thus have clear, accessible and prominent reporting features. Many of these reporting features will be within the profiles themselves, so they are 'handy' for the user. If social network sites do receive reports about cyber-bullying, they will investigate and can remove content that is illegal or break their terms and conditions in other ways. They can delete the account of those who have broken the rules.

Video-hosting Sites

It is possible to get content taken down from video-hosting sites, though the content will need to be illegal or have broken the terms of service of the site in other ways. On YouTube, perhaps the most well-known of such sites, it is possible to report content to the site provider as inappropriate. In order to do this, you will need to create an account (this is free) and log in, and then you will have the option to 'flag content as inappropriate'. The option to flag the content is under the

video content itself. YouTube provides information on what is considered inappropriate in its terms of service. See www.youtube.com/t/terms