e-Safety Policy

Policy intended for:	Staff
Category:	IT Policy
Published:	Server, Policy folders at College and Student Accommodation, Staff handbook
Policy Implemented by:	Principal, Operations Manager, IT & MIS Coordinator
Policy Monitored by:	Principal and Operations Manager
Reviewed by:	Principal
Reviewed date:	January 2020
Consultation with:	Senior Leadership Team (SLT)
Record of changes & additions:	22 Dec 17 changed he/she to them 20 Feb, included Operations Manager and IT & MIS Co-ordinator to persons implementing policy. Operations Manager now the e-Safety Co-ordinator Jan 20: None
Next Review	August 2020

Introduction

This e-Safety policy recognises our commitment to e-safety and acknowledges its part in the College's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep students safe.

We believe our whole College community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities.

As part of our commitment to e-Safety we also recognise our obligation to implement a range of security measures to protect the College network and facilities from attack, compromise and inappropriate use and to protect College data and other information assets. We have adopted the good practice requirements for all staff which are included in the **Staff / Tutor Handbook.**

For the purposes of clarity and consistency throughout this document the person in Oxford International College who is taking a lead on e-Safety is called the **e-Safety Coordinator.**

The person at Oxford International College taking on the role of e-Safety Coordinator is **The Operations Manager.**

This policy applies to the use of all electronic devices used to access the internet, including desktop computers, laptops, tablets and smartphones.

Responsibilities of the College Community

We believe that e-Safety is the responsibility of the whole College community and that everyone has their part to play in ensuring all members of the College community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the College community can contribute.

The SLT accepts the following responsibilities:

- To identify a person (the e-Safety coordinator) to take responsibility for e-Safety and support them in their work.
- Ensure adequate technical support is in place to maintain a secure IT system
- Ensure policies and procedures are in place to ensure the integrity of the College's information and data assets
- Develop and promote an e-Safety culture within the College community
- Ensure that all staff and students agree to abide by the **Internet, Email and Telephone Policy** and that new staff have e-Safety included as part of their College induction procedures
- Make appropriate resources, training and support available to all members of the College community to ensure they are able to carry out their roles effectively with regard to e-Safety
- Receive and regularly review e-Safety incident logs; ensure that the correct procedures are followed should an e-Safety incident occur in College and review incidents to see if further action is required
- To take ultimate responsibility for the e-Safety of the College community

The responsibilities of the e-Safety Coordinator are:

- To promote an awareness and commitment to e-Safety throughout the College
- To be the first point of contact in College on all e-Safety matters
- To lead College e-Safety meetings which are part of the regular IT meetings
- To create and maintain e-Safety policies and procedures
- To develop an understanding of current e-Safety issues, guidance and appropriate legislation
- To ensure delivery of an appropriate level of training in e-Safety issues
- To ensure that e-Safety education is embedded across the curriculum
- To ensure that any person who is not a member of College staff, who makes use of the College IT equipment in any context, is made aware of the **Internet, Email and Telephone Policy.**
- To liaise with the Local Authority, Oxford Safeguarding Children's Board and other relevant agencies as appropriate
- To monitor and report on e-Safety issues to the Senior Leadership Team
- To ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable or that contravenes this ePolicy
- To ensure an e-Safety incident log is kept and up to date
- To ensure that the **Internet Email and Telephone Policy** and **e-Safety Policy** are displayed in appropriate areas around the site
- The responsibilities of all staff are:
- To read, understand and help promote the College's **Internet Email and Telephone Policy**
- To take responsibility for ensuring the safety of sensitive College data and information
- To develop and maintain an awareness of current e-Safety issues and legislation and
- guidance relevant to their work
- To maintain a professional level of conduct in their personal use of technology at all times
- To embed e-Safety messages in learning activities where appropriate
- To supervise students carefully when engaged in learning activities involving technology
- To ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- To report all e-Safety incidents which occur in the appropriate log and/or to their line manager
- To respect the feelings, rights, values, beliefs and intellectual property of others in their use of technology in College and at home

The responsibilities of all students are:

- To take responsibility for their own use of technology at all times
- To ensure they respect the feelings, rights, values, beliefs and intellectual property of others in their use of technology in College and outside of College
- To understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology, or if they know of someone to whom this is happening
- To report all e-Safety incidents to appropriate members of staff
- To discuss e-Safety issues with family and friends in an open and honest way

Learning and Teaching

Oxford International College believes that the key to developing safe and responsible behaviours online for everyone within our College community lies in effective education. We know that the Internet and other technologies are embedded in our students' lives, not just in College but outside as well, and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present.

We believe that learning about e-Safety should be embedded across the curriculum and also taught in specific sessions such as evening seminars.

We will discuss, remind or raise relevant e-Safety messages with students routinely wherever suitable opportunities arise.

Managing and Safeguarding IT Systems

The College will ensure that access to the College IT system is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure are located securely with only appropriate staff permitted access. Servers, workstations and other hardware and software are kept updated as appropriate. A firewall is maintained and virus and malware protection is installed on all appropriate hardware and is kept active and up-to-date. Staff have virus protection installed on all laptops used for College activity.

Any administrator or master passwords for College IT systems are kept secure.
Any future wireless network is protected by a secure log on which prevents unauthorised access.
New users can only be given access by nominated individuals.

We do not allow anyone except technical staff and staff with administrator rights to download and install software onto the network.

Filtering Internet access
Web filtering of internet content is provided by through our Firewall. This ensures that all reasonable precautions are taken to prevent access to inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur. Teachers are encouraged to check out websites they wish to use. All users are informed about the action they should take if inappropriate material is accessed or discovered on a computer.

Access
The College decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are security systems in place for managing network accounts and passwords, including safeguarding administrator passwords.
Staff are given appropriate guidance on managing access to laptops which are used both at home and College.

Access to personal, private or sensitive information and data is restricted to authorised users only, with proper procedures being followed for authorising and protecting login and password information.

Remote access to College systems is covered by specific agreements and must never be allowed to be used by an unauthorised third-party user.

Using the Internet

We provide the internet to:

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the College's management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the examination boards and others

Users are made aware that they must take responsibility for their own use of and their behaviour whilst using the College IT systems or a College provided device and that such activity can be monitored and checked.

All users of the College IT or electronic equipment will abide by the relevant **Internet, Email and Telephone Policy** at all times, whether working in a supervised activity or working independently.

Students and staff are made fully aware of the actions that will be taken if inappropriate material is discovered and the consequences that these findings may involve.

Using Email

Email is regarded as an essential means of communication and the College provides all members of the College community with an e-mail account upon request. Communication by email between staff and students/parents will only be made using the College email account and should be professional and related to College matters only. Email messages on College business should be regarded as having been sent on headed notepaper and reflect a suitable tone and content and should ensure that the good name of the College is maintained. There are systems in place for storing relevant electronic communications which take place between College and parents.
Use of the College Email system is monitored and checked.
Responsible use of personal web mail accounts by staff is permitted.

Publishing content online on the College website:
The College maintains editorial responsibility for any College initiated web site or learning platform content to ensure that content is accurate and the quality of presentation is maintained. The College maintains the integrity of the College web site by ensuring that responsibility for uploading material is always moderated and that passwords are protected.

Identities of students are protected at all times. The College obtains permission from parents for the use of students' photographs. Group photographs do not have a name list attached.

Creating online content as part of the curriculum:
As part of the curriculum we encourage students to create online content. Students are taught safe and responsible behaviour in their creation and publishing of online content. They are taught to publish for a wide range of audiences which might include governors, parents/guardians or younger children.

We take all steps to ensure that any material published online is the author's own work, gives credit to any other work included and does not break copyright rules.

Online material published outside the College:
Staff and students are encouraged to adopt similar safe and responsible behaviours in their personal social networking sites and other online publishing outside College as they are in College.

Material published by students, tutors and staff in a social context which is considered to bring the College into disrepute or considered harmful to, or harassment of another student or member of the College community will be considered a breach of College discipline and treated accordingly.

Using images, video and sound
We recognise that many aspects of the curriculum can be enhanced by the use of multi-media and that there are now a wide and growing range of devices on which this can be accomplished.

Students are taught safe and responsible behaviour when creating, using and storing digital images, video and sound.

Digital images, video and sound recordings are only taken with the permission of participants; images and video are of appropriate activities and are only taken of students wearing appropriate dress. Full names of participants are not used either within the resource itself, within the file-name or in accompanying text online.

College performances, debates, shows, etc may be recorded. However, students will be consulted before the recording etc takes place. No student’s role or part in any performance or event would be jeopardised because they do not want to be photographed or recorded.

Using other technologies
As a College we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-Safety point of view.

We will review the e-Safety policy when necessary or due to the introduction of any new technology that may not be covered by this policy.

Staff or students using a new technology not specifically mentioned in this policy will be expected to behave with similar standards of behavior to those outlined within this document.

Protecting College data and information

OXFORD INTERNATIONAL COLLEGE recognises its obligation to safeguard staff and student's personal data including that which is stored and transmitted electronically. We regularly review our practices and procedures to ensure that they meet this basic obligation.

The College is a registered Data Controller under the Data Protection Act 1998 and we comply at all times with the requirements of that registration.

Suitable procedures, and where necessary training, are in place to ensure the security of such data including the following:

- All devices holding sensitive information are password protected and staff are aware that all computers must be locked when they are left unattended
- Staff are provided with appropriate levels of access to the College's management information system (ENGAGE) holding student data. Passwords are not shared and administrator passwords are kept by each member of staff individually
- Staff are aware of their obligation to keep sensitive data secure when working on computers outside College
- When we dispose of old computers and other equipment we take due regard for destroying information which may be held on them
- We have full back up and recovery procedures in place for College data
- Sensitive staff or student data is only accessible to people who have a right to see the information, and they are reminded on receiving the information of their duty to keep it safe and secure and that it is not to be seen or discussed with any third party.

Dealing with e-Safety incidents

All e-Safety incidents should be recorded in the College e-Safety Log which should be regularly reviewed.

Any incidents where students do not follow the **Internet Email and Telephone Policy** will be dealt with following the College's normal behaviour or disciplinary procedures.

In situations where a member of staff is made aware of a serious e-Safety incident, concerning students or staff, they will inform the e-Safety coordinator or if necessary the college Safeguarding Officer (Kim Terrar), who will then respond in the most appropriate manner.

Instances of **cyberbullying** will be taken very seriously by the College and dealt with using the Colleges anti-bullying procedures. The College recognises that staff as well as students may be victims and will take appropriate action in either situation.

Cyberbullying will not be tolerated.

Incidents which create a risk to the security of the College network, or create an information security risk, will be referred to the College's e-Safety Coordinator and technical support and appropriate advice sought and action taken to minimize the risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches College policy then appropriate sanctions will be applied. The College will decide if parents need to be informed if there is a risk that student data has been lost.

College reserve the right to monitor equipment of their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with a Child Protection issue arising from the use of technology:
If an incident occurs which raises concerns about Child Protection or the discovery of indecent images on the computer, then the procedures outlined in the Safeguarding Procedures will be followed.

Dealing with complaints and breaches of conduct by students:

- Any complaints or breaches of **Internet, Email and Telephone Policy** will be dealt with promptly under the College discipline system
- Responsibility for handling serious incidents will be given to a senior member of staff
- An initial fact finding investigation must be carried out
- Parents and the student will work in partnership with staff to resolve any issues arising
- There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies. External agencies will be contacted as appropriate

The following activities constitute behavior which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene,
- defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned, any form of cyberbullying will not be tolerated
- using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action:

- any online activity by a member of the College community which is likely to adversely impact on the reputation of the College
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at College or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using College or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the College into disrepute
- attempting to circumvent filtering, monitoring or other security systems
- circulation of commercial, advertising or 'chain' emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data protection Act, revised 1988

- accessing social networking sites, chat sites, instant messaging accounts, email or using a mobile phone for personal use during lesson time
- accessing non-educational websites (e.g. gaming or shopping websites) during lesson time
- sharing a username and password with others or allowing another persona to log in using your account
- accessing College IT systems with someone else's username and password
- deliberately opening, altering, deleting or otherwise accessing files or data belonging to someone else

Appendix

Extract from:

Guidance for the Safer Working Practice for Adults who work with Children and Young People.

Section 12 Communication with Children and Young People *(including the Use of Technology)* Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny.

Adults should also be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/guardians. E-mail or text communications between an adult and a child young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet-based web sites.

Communication systems should only be used in accordance with the Colleges policies.

This means that the College should have a communication policy which specifies acceptable and permissible modes of communication underlining to staff that they should:

- never give their personal contact details to a children or young people, including their mobile telephone number and details of any blogs or personal websites
- only use communication equipment e.g. mobile phones, provided by the college for work purposes and never to communicate with students or young persons
- only make contact with children for professional reasons and in accordance with any college policy as part of your work commitment
- be aware of the inappropriate forms of contact with a student at all times
- not use internet or web-based communication channels to send personal messages to a child or young person e.g. Facebook

Photography and Videos

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well being of children and young people. Informed written consent from parents/guardians and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose.

Careful consideration should be given as to how activities involving the taking of images are organised and undertaken. Care should be taken to ensure that all parties understand the implications of the image being taken especially if it is to be used for any publicity purposes or published in the media, or on the Internet. There also needs to be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.

Adults need to remain sensitive to any children who appear uncomfortable, for whatever reason, and should recognise the potential for such activities to raise concerns or lead to misunderstandings.

It is not appropriate for adults to take photographs of children for their personal use.

This means that staff should:

- be clear about the purpose of the activity and about what will happen to the images when the activity is concluded
- be able to justify any images of children
- avoid making images in one to one situations or which show a single child with no surrounding context
- ensure the child/young person understands why the images are being taken and has agreed to the activity and that they are appropriately dressed.
- only use equipment provided or authorised by the college
- report any concerns about any inappropriate or intrusive photographs found
- always ensure they have parental permission to take and/or display photographs of a student/child
- This means that adults should not:
- display or distribute images of children unless they have consent to do so from parents/guardians
- use images which may cause distress
- use mobile telephones (College or personal) to take images of children
- never take images 'in secret' or taking images in situations that may be construed as being secretive.

Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of children. Adults 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 on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven.

Adults should not use equipment belonging to the college to access adult 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. Adults should ensure that children and young people are not exposed to any inappropriate images or web links. Oxford International College needs to ensure that internet equipment used by children have the appropriate controls with regards to access. e.g. personal passwords should be kept confidential.

Where indecent images of children or other unsuitable material are found, the **Designated Safeguarding Lead Officer** must be informed immediately. He/she will then inform the **Police and Local Authority Designated Officer (LADO)**. At **no** time should anyone 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.

This means that the College should:

- have a clearly defined Internet Code of Conduct Policy
- have clear e-safety policies in place about access to and use of the internet
- make guidance available to both staff, children and young people about appropriate usage.
- This means that staff should:
- adhere to the Internet, Email and Telephone Policy
- follow the guidance on the **Use of IT** equipment
- ensure that children are not exposed to unsuitable material on the internet
- ensure that any films or material shown to children and young people are age appropriate.

.

Further information

If you have any questions about e-Safety at Oxford International College, please contact:

Claire.wellstood@oxcoll.com
Operations Manager
Oxford International College
1 London Place
Oxford
OX4 1BD