Britannica International, Shanghai

Online Safety Policy

1988 Gubei Road, Shanghai 201103 China Telephone: 021 6402 7889
principal@britannicashanghai.com
www.britannicashanghai.com

August 2021

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by a working group / committee made up of: *(SLT, DSL, Friends of Britannica, students and teaching staff)*

- Principal / Senior Leaders
- Online Safety Officer / Coordinator
- Staff – including Teachers, Support Staff, Technical staff
- Regional Head of Schools/ Board
- Parents
- Student Council

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Board	*Insert date*
The implementation of this Online Safety policy will be monitored by the:	*Senior Leadership Team and other DSL*
Monitoring will take place at regular intervals:	*End of Terms 1, 2 and 3*
The Regional Head of Schools/ Group Head of IT and the Board will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually unless there are incidents of concern which would necessitate an immediate report. Reportable incidents would also be raised in the Principal's Monthly Report.
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	July 2022
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Regional Head of Schools and the Group Head of IT. Infringement of the law would be referred to the appropriate authority.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

UK ref The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers about the searching for and of electronic devices and the deletion of data In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within *the school*: (In smaller *schools* some of the roles described below may be combined, though it is important to ensure that there is sufficient "separation of responsibility" should this be the case).

Regional Head of Schools (RHoS) acting on behalf of the Board of Directors

The Board is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the RHoS receiving regular information about online safety incidents and monitoring reports. The RHoS has taken on the role of *Online Safety Operational Board member* (it is suggested that the role may be combined with that of the Head Office Designated Lead on Safeguarding and Child Protection). The role of the *Online Safety Operational Board member will include*:

- regular meetings with the Online Safety Co-ordinator/ Designated Safeguarding Lead / Principal
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Board meeting

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the *Designated Safeguarding Lead* (DSL) Deputy *Designated Safeguarding Lead* (DDSL)
- The Principal and (at least) one another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents).
- The Principal / Senior Leaders are responsible for ensuring that the Online Safety Officer / Lead and other relevant staff receive suitable training to enable them to carry out their online 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 online safety monitoring role. This is to provide a safety net and support those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the *Designated Safeguarding Lead* (DSL) Deputy *Designated Safeguarding Lead* (DDSL)

Online Safety Officer / Lead (DSL or DDSL)

(It is **strongly recommended** that each school should have a named member of staff with a day to day responsibility for Online Safety, some schools may choose to combine this with the Designated Safeguarding Lead (DSL/ DDSL) role. Schools may choose to appoint a person with a child welfare background, preferably with good knowledge and understanding of the new technologies, rather than a technical member of staff – but this will be the choice of the school)

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- where necessary liaises with the municipal authority
- liaises with school technical staff

- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments, (Examples of suitable log sheets may be requested from Orbital Head Office)
- where necessary meets regularly with Online Safety Board member to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

(The school will need to decide how these incidents will be dealt with and whether the investigation / action / sanctions will be the responsibility of the Online Safety Officer / Lead or another member of staff e.g. Principal / Senior Leader / Designated Safeguarding Lead / Class teacher / Head of Year.)

Network Manager / Technical staff

(nb. if the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy and procedures.)

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any national /municipal / other relevant body Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network / internet / Learning Platform / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Principal / Designated Safeguarding Lead* (DSL) Deputy *Designated Safeguarding Lead* (DDSL)
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- **they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Principal *Designated Safeguarding Lead (DSL/ DDSL insert others as relevant)* for investigation / action / sanction**

- **all digital communications with students and parents should be on a professional level *and only carried out using official school systems, it is forbidden to communicate with students or parents using the WeChat platform***
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies regarding 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

Designated Safeguarding Lead / Designated Person

Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding 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
- online-bullying

(n.b. it is important to emphasise that these are safeguarding issues, not technical issues, simply that the technology provides additional means for safeguarding issues to develop. Some schools may choose to combine the roles of Designated Safeguarding Lead and Online Safety Officer).

Optional Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from *the school* community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. Depending on the size or structure of the school this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Principal.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Officer / Lead (or another relevant person, as above) with:

- the review / monitoring of the school Online Safety Policy / documents.

- mapping and reviewing the online safety / digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents and the students about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

(Schools will need to decide the membership of the Online Safety Group. It is recommended that the group should include representation from students and parents. An Online Safety Group Terms of Reference Template may be requested from Orbital Head Office).

Students:

- **are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement**
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. *The* school will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website / Learning Platform and information about national / local online safety campaigns / literature*. Parents will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / Learning Platform and on-line student records
- *their children's personal devices in the school (where this is allowed)*
- *BYOD online safety lessons and workshops with both students and parents*

Community Users

Community Users who access school systems / website / Learning Platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems. (A Community Users Acceptable Use Agreement Template may be requested from the Head Office).

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety / digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- **A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.**
- *Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that 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.*
- *Where students can freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents

Many parents have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and through:

- *Curriculum activities*
- *Letters, newsletters, web site, Learning Platform*
- *Parents evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g. www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers*

Recommended Education – The Wider Community (Partnerships)

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *The school website will provide online safety information for the wider community*
- *Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision*
- Use of medical insurance provider to source professionals for lectures, workshops, symposiums etc.

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select / delete as appropriate)

- **A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.**
- **All new staff should receive online safety training (EduCare- Online Safety for International Schools) as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.**
- **This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.**
- *The Online Safety Officer / Lead (or other nominated person) will provide advice / guidance / training to individuals as required.*

Training – Regional Head of Schools and Board

Board members should take part in online safety training / awareness sessions, with importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in several ways:

- Training provided by the Group Head of IT
- Participation of online training provided by relevant organisation such as EduCare.
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school Online Safety Policy / Acceptable Use Agreements.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: (schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:) A review of this section will take place week beginning 16th August when all involved staff return

(A more detailed Technical Security Template Policy may be requested from Orbital Head Office)

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**

- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users** (*at KS1 and above*) **will be provided with a username and secure password by** (IT manager *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change their password every Term* (Schools may choose to use group or class log-ons and passwords for KS1 and below, but should consider whether this models good password practice and need to be aware of the associated risks)
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or another person) must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. school safe)
- The IT manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the **Internet Watch Foundation CAIC** list. Content lists are regularly updated, and internet use is logged and regularly monitored. (the school will need to decide on the merits of external / internal provision of the filtering service).
- **Additional filters to be used in the event of VPN allowing inappropriate content to bypass initial filtering software**
- **Internet filtering / monitoring should ensure that children are safe from radicalisation material when accessing the internet.**
- *The school has provided enhanced / differentiated user-level filtering* (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc)
- *School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement*
- *An appropriate system is in place, where Director of EdTech, Principal and IT manager are informed,for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

- *An agreed policy is in place* (to be described) *regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place* (to be described) *that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place* (to be described) *regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured****.*
- All to be described sections to be populated following relevant staff returning and meeting

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network, filtering of personal devices, breakages and insurance, access to devices for all students, avoiding potential classroom distraction, network connection speeds, types of devices, charging facilities, total cost of ownership. A range of mobile technology implementations is possible

(A more detailed Mobile Technologies Template Policy may be requested from Orbital Head Office).

The school may however choose to include these aspects of their policy in a comprehensive Acceptable Use Agreement, rather than in a separate Mobile Technologies Policy. It is suggested that the school should in this overall policy document outline the main points from their agreed policy.

A checklist of points to be considered in included below.

- **The school Acceptable Use Agreements for staff, students and parents will consider the use of mobile technologies**
- **The school allows:** (the school should complete the table below to indicate which devices are allowed and define their access to school systems)

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes/No[2]*	*Yes/No[2]*	*Yes/No[2]*
Full network access	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*No*
Internet only	*No*	*No*	*No*	*Yes*	*Yes*	*Yes*
No network access						

Aspects that the school may wish to consider and be included in their Online Safety Policy, Mobile Technologies Policy or Acceptable Use Agreements:

School owned / provided devices:

- *Who they will be allocated to*
- *Where, when and how their use is allowed – times / places / in school / out of school*
- *If personal use is allowed*
- *Levels of access to networks / internet (as above)*
- *Management of devices / installation of apps / changing of settings / monitoring*
- *Network / broadband capacity*
- *Technical support*
- *Filtering of devices*
- *Access to cloud services*
- *Data Protection*
- *Taking / storage / use of images*

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

[2] The school should add below any specific requirements about the use of mobile / personal devices in school

- *Exit processes – what happens to devices / software / apps / stored data if user leaves the school*
- *Liability for damage*
- *Staff training*

Personal devices:

- Which users can use personal mobile devices in school (staff / students / visitors)
- Restrictions on where, when and how they may be used in school
- Storage
- Whether staff will be allowed to use personal devices for school business
- Levels of access to networks / internet (as above)
- Network / broadband capacity
- Technical support (this may be a clear statement that no technical support is available)
- Filtering of the internet connection to these devices
- Data Protection
- Taking / storage / use of images
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- Identification / labelling of personal devices
- How visitors will be informed about school requirements
- How education about the safe and responsible use of mobile devices is included in the school Online Safety education programmes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: (select / delete as appropriate)

- **When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents will be obtained before photographs of students are published on the school website / social media / local press** (may be covered as part of the AUA signed by parents or carers at the start of the year - see Parents Acceptable Use Agreement available from Head Office)
- In accordance with guidance from the UK Information Commissioner's Office (Principals should seek clarification on legal requirements/ legislation of host country), parents are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images **should not** be published / made publicly available on social networking sites, **nor should parents** comment on any activities involving other students in the digital / video images.
- Staff and volunteers can take digital / video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available from Orbital Head Office.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- **It has a Data Protection Policy. (this may be requested from Orbital Head Office)**

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay.**
- **The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in a Privacy Notice.**
- **Where special category data is processed, a lawful basis and a separate condition for processing have been identified.**
- **Data Protection Impact Assessments (DPIA) are carried out.**
- **It has clear and understood arrangements for access to and the security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers.**
- **Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller.**
- **There are clear and understood data retention policies and routines for the deletion and disposal of data.**
- **There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible.**
- **Consideration has been given to the protection of personal data when accessed using any remote access solutions.**
- **All schools / academies (n.b. including Academies, which were previously exempt) must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **All staff receive data handling awareness / data protection training and are made aware of their responsibilities.**

Staff must ensure that they:

- **At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- **The data must be encrypted, and password protected.**

- The device must be password protected. (many memory sticks / cards and other mobile devices cannot be password protected)
- **The device must offer approved virus and malware checking software.**
- **The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.**

(The school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices.)

Communications

This is an area of rapidly developing technologies and uses. Schools will need to discuss and agree how they intend to implement and use these technologies e.g. some schools do not allow students to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students. The table has been left blank for school to choose its own responses.

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults			Students / Pupils				
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school / academy	x				x			
Use of mobile phones in lessons		x				x		
Use of mobile phones in social time	x							x
Taking photos on mobile phones / cameras		x					x	
Use of other mobile devices e.g. tablets, gaming devices	x				x			
Use of personal email addresses in school or on school network				x				x
Use of school email for personal emails				x				x
Use of messaging apps	x					x		
Use of social media	x					x		
Use of blogs	x				x			

Orbital would strongly recommend that schools do include the following statements:

The school may also wish to add some of the following policy statements about the use of communications technologies, in place of, or in addition to the above table:

When using communication technologies, the school considers the following as good practice:

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and students should therefore use only the school email service to communicate with others when in school, or on school / systems (e.g. by remote access).*
- **Users must immediately report, DSL/DDSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and students or parents (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while students at KS2 and above will be provided with individual school email addresses for educational use.* (Schools may choose to use group or class email addresses for younger age groups e.g. at KS1)
- ***Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.***
- ***Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.***

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of students, the school and the individual when publishing any material online. **Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012' (which Orbital Schools have either incorporated into their Staff Code of Conduct or have as a 'standalone' Teacher Standards Policy). Ofsted's online safety inspection framework and CIS/ COBIS accreditation standards reviews how a school protects and educates staff and students in their use of technology, including the measures that would be expected to be in place to intervene and support should an issue arise.** Schools increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

A more detailed Social Media Template Policy is available from Orbital Head Office. The school may however choose to include these aspects of their policy in a comprehensive Acceptable Use Agreement, rather than in a separate Social Media Policy. It is suggested that the school should in this overall policy

document outline the main points from their agreed policy. A checklist of points to be considered is included below.

All schools have a duty of care to provide a safe learning environment for students and staff. Schools could be held responsible, indirectly for acts of their employees during their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

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

School staff should ensure that:

- No reference should be made in social media to students, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Orbital Education
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

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

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

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- **The school permits reasonable and appropriate access to private social media sites**

Monitoring of Public Social Media

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

The school's use of social media for professional purposes will be checked regularly by the DSL/DDSL/IT Manager to ensure compliance with the school policies.

Dealing with unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			x		
On-line gaming (non-educational)				x	
On-line gambling					x
On-line shopping / commerce				x	
File sharing			x		
Use of social media -see above			x		
Use of messaging apps			x		
Use of video broadcasting e.g. YouTube			x		

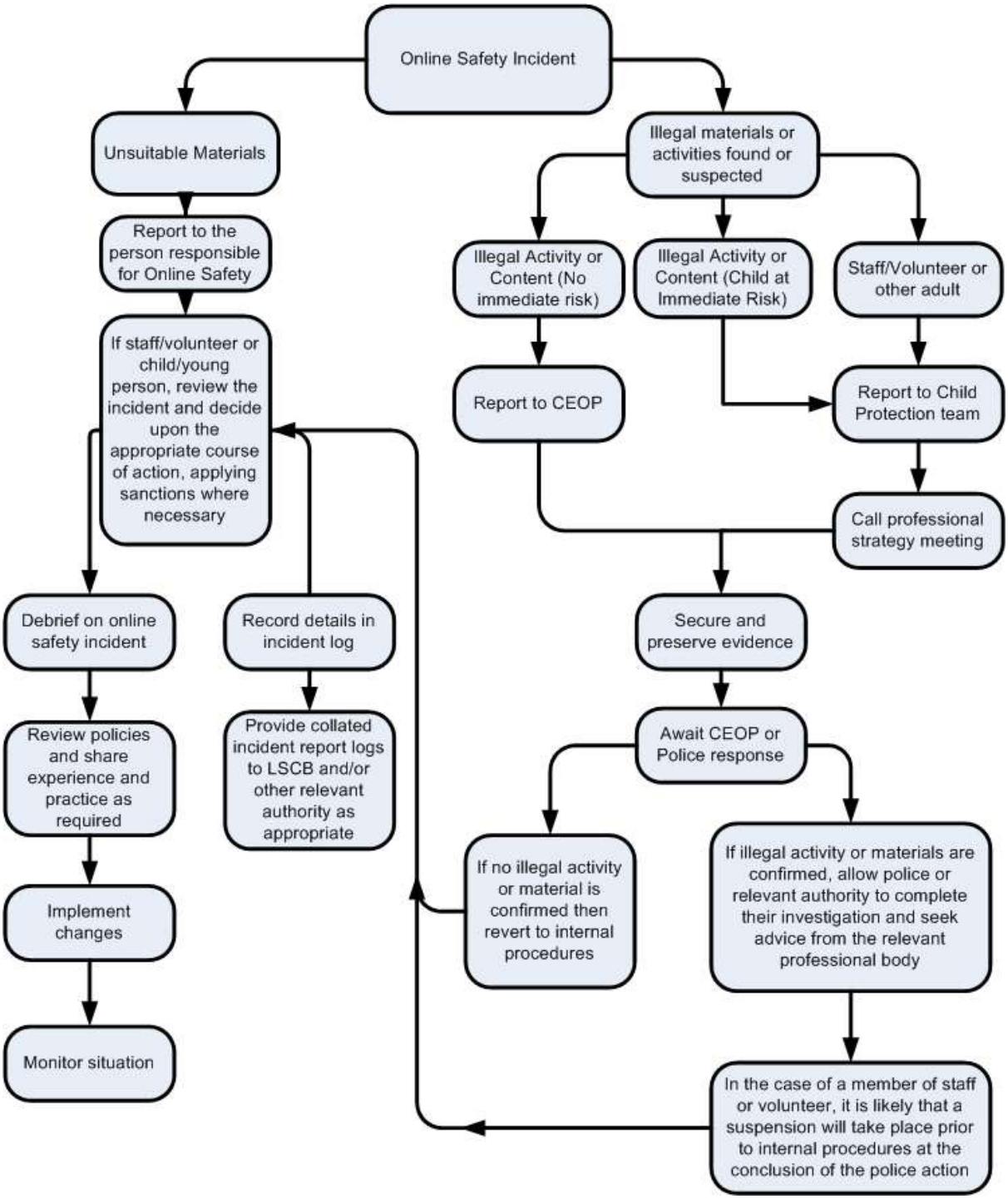
(The school should agree its own responses and place the ticks in the relevant columns, in the table above. They may also wish to add additional text to the column(s) on the left to clarify issues. The last section of the table has been left blank for schools to decide their own responses)

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. **These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)**
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the Regional Head of Schools/ Group or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Regional Head of Schools and Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings / training sessions).

Actions / Sanctions

Students Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	x								

Unauthorised / inappropriate use of mobile phone / digital camera / another mobile device	x								
Unauthorised / inappropriate use of social media / messaging apps / personal email	x								
Unauthorised downloading or uploading of files	x								
Allowing others to access school network by sharing username and passwords	x	x							
Attempting to access or accessing the school network, using another student's account	x	x							
Attempting to access or accessing the school network, using the account of a member of staff	x	x	x	x					x
Corrupting or destroying the data of other users	x	x	x	x					x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x		x			x
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x		x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x	x		x	x		x
Using proxy sites or other means to subvert the school's filtering system	x	x	x	x		x	x		x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x		x	x		
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x		x	x		x

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x		x	x		x

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Principal	Refer to RHoS / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	x							
Unauthorised downloading or uploading of files	x							
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x	x					
Careless use of personal data e.g. holding or transferring data in an insecure manner	x							
Deliberate actions to breach data protection or network security rules	x	x						x

Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x					x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x					x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students	x	x	x		x			x
Actions which could compromise the staff member's professional standing	x	x						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x					x
Using proxy sites or other means to subvert the school's filtering system	x	x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x					
Deliberately accessing or trying to access offensive or pornographic material	x	x	x		x			x
Breaching copyright or licensing regulations	x	x						
Continued infringements of the above, following previous warnings or sanctions	x	x	x		x			x

Review and Evaluation

This policy is to be review annually, though any deficiencies or weaknesses in policy arrangements will be remedied without delay.

This policy will be reviewed by the Principal and leadership team.

Drafted: July 2018
Reviews: August 2021