Digital Safeguarding Policy

Policy Version Control

Policy type	Academy Mandatory Policy
Policy prepared by (name and department)	Iain Smith, E-Safety Co-ordinator
Last review date	September 2017
Date of approval	December 2017
Approved by	Jane Dickens, Vice Principal
Date released	December 2017
Next review date	September 2018

1.1 Policy Statement

Ormiston SWB Academy recognises that ICT and the internet are fantastic tools for learning and communication that can be used in the Academy to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the Academy community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the Academy community are aware of the dangers of using the internet and how they should conduct themselves online. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. E-safety covers the internet but it also covers mobile phones and other electronic communications technologies.

1.2 Policy Aims

This policy aims to be an aid in regulating ICT activity in the Academy, and provide a good understanding of appropriate ICT use that members of the Academy community can use as a reference for their conduct online outside of the Academy hours. E-safety is a whole-Academy issue and responsibility. In addition, there is a 'duty of care' for any persons working with children and educating all members of the Academy community on the risks and responsibilities of e-safety falls under this duty, the policy aims to highlight this duty. With the increase of terrorist and extremist content online growing daily, the policy will provide guidance on what the Academy does to prevent access to such material.

1.3 Key Personnel

Principal	• Ensure that the Digital Safeguarding Policy is implemented and compliance with the policy monitored, and that the appropriate roles (see this section) and responsibilities of the Academy digital safeguarding structure is in place. Ensure regular reports of the monitoring outcomes on digital safeguarding are reported to the Governing Body.
Vice Principal (Behaviour & Safety) Child Protection Officer	• The Child Protection Officer will be the first point of contact with any concerns with regards to Safeguarding; they will assess the concern and take the appropriate action needed. CPO will ensure that all staff are familiar with and adhere to the Academy Safeguarding Policies. • Responsible for e-safety developments in the Academy and sharing of practice with staff and the wider community. • Will be in receipt of current training on the latest guidance and procedures. • Main contact for the Local Authority e-Safety networks. • All digital safeguarding incidents within the Academy need to be reported to this person. Keep the log of incidents and with the Principal or CPO make decisions about how to deal with reported incidents.
E-safety Co-ordinator	• Ensure up-to-date with latest developments and issues of concern, publicising these appropriately to staff, students and parents. • Be in receipt of all digital safeguarding concerns and liaise immediately with the Principal/CPO where concerns are related to Child Protection. • Keep logs of any reported incidents and actions taken to resolve these. • Have the appropriate training for this level of post.

Academy Staff	• All staff with subject and management roles have a duty to incorporate e-safety principles in their area of responsibility. • All staff will understand the need for care and caution when using technology both for academic and social purposes and apply it to teaching and learning situations. • All staff need to work to agreed guidelines and have a "front line" monitoring and reporting role for incidents. • Any concerns should be reported to the e-safety co-ordinator.

Policy Specific Statements and Principles

Communicating Academy policy

This policy is available from the Academy E-safety Co-ordinator and on the Academy website for parents, staff, and students to access when and as they wish. Rules relating to the Academy code of conduct when online, and e-safety guidelines, are displayed around the Academy. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHEE lessons and assemblies where personal safety, responsibility, and/or development are being discussed.

Making use of ICT and the internet in the Academy

The internet is used in the Academy to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the Academy's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave the Academy. Some of the benefits of using ICT and the internet in the Academy are:

For students:

- Unlimited access to worldwide educational resources/institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between students all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to explore the world and its cultures from within a classroom. Freedom to be creative.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.
- Class management, attendance records, schedule, and assignment tracking.

For parents:

- Ability to engage in their child's learning through access to Academy online systems.
- Up to date Academy correspondence through the texting service, social media and Go4Schools.

Learning to evaluate internet content

With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the Academy across all subjects in the curriculum. Students will be taught: to be critically aware of materials, and shown how to validate information before accepting it as accurate; to use age-appropriate tools to search for information online; to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the Academy will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined. If they have plagiarised in an exam or a piece of coursework, they may be prohibited from completing that exam.

The Academy will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the Academy e-safety co-ordinator and ICT Support Team. Any material found by members of the Academy community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

Managing information systems

The Academy is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of Academy data and personal protection of our Academy community very seriously. This means protecting the Academy network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by Network Manager and virus protection software will be updated regularly. Some safeguards that the Academy takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted
- making sure that unapproved software is not downloaded to any Academy computers. Alerts will be set up to warn users of this
- files held on the Academy network will be regularly checked for viruses
- the use of user logins and passwords to access the Academy network will be enforced
- portable media containing Academy data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

For more information on data protection in the Academy please refer to our **data protection policy**. More information on protecting personal data can be found in **section 11** of this policy.

Emails

The Academy uses email internally for staff and students, and externally for contacting parents, and is an essential part of the Academy communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and students should be aware that Academy email accounts should only be used for Academy-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The Academy has the right to monitor emails and their contents but will only do so if it feels there is reason to.

Academy email accounts and appropriate use

Staff should be aware of the following when using email in the Academy:

- Staff should only use official Academy-provided email accounts to communicate with students, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during Academy hours.

- Emails sent from Academy accounts should be professionally and carefully written. Staff are representing the Academy at all times and should take this into account when entering into any email communications.
- Staff must tell their line manager or a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the Academy or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in the Academy.

Students should be aware of the following when using email in the Academy, and will be taught to follow these guidelines through the ICT curriculum and in any instance where email is being used within the curriculum or in class:

- in the Academy, students should only use Academy-approved email accounts
- excessive social emailing will be restricted
- students should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the Academy or from an external account. They should not attempt to deal with these themselves.
- students must be careful not to reveal any personal information over email, or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
- Students will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the Academy network or their personal account or wellbeing.

Published content and the school website

The Academy website is viewed as a useful tool for communicating our Academy ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with Academy news and events, celebrating whole-Academy achievements and personal achievements, and promoting Academy projects.

The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the Academy community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the Academy will be for the Academy office only. **For information on the Academy policy on children's photographs on the Academy website please refer to the section below.**

Policy and guidance of safe use of children's photographs and work

Colour photographs and students work bring our Academy to life, showcase our student's talents, and add interest to publications both online and in print that represent the Academy. However, the Academy acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without consent. On admission to the Academy parents/carers will be asked to sign a photography consent form. The Academy does this so as to prevent repeatedly asking parents for consent over the Academy year, which is time-consuming for both parents and the Academy. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the Academy's policy on the use of photographs of children, including:

- how and when the photographs will be used
- how long parents are consenting the use of the images for
- Academy policy on the storage and deletion of photographs.

Parents will be asked for consent when their child joins the Academy.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place to deal with any potential issues.

Only images created by or for the Academy will be used in public and children may not be approached or photographed while in the Academy or doing Academy activities without the Academy's permission. The Academy follows general rules on the use of photographs of individual children.
Parental consent must be obtained. Consent will cover the use of images in:

- all Academy publications
- on the Academy website
- in newspapers as allowed by the Academy
- in videos made by the Academy or in class for Academy projects.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities); will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names may be used on public documents and published alongside images of the child. Groups may be referred to collectively by year group, form name or named individually with their full name.
- Events recorded by family members of the students such as Academy plays or sports days must be used for personal use only.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
- Any photographers that are commissioned by the Academy will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in the Academy please refer to our **Academy child protection and safeguarding policy.**

Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of Academy photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the Academy **child protection and safeguarding** policy and **behaviour policy.**

Extremism and radicalism

What is meant by Extremism and Radicalism?
Radicalisation is defined as the act or process of making a person more radical or favouring of extreme or fundamental changes in political, economic or social conditions, institutions or habits of the mind.
Extremism is defined as the holding of extreme political or religious views.

Although serious incidents involving radicalisation have not occurred at Ormiston SWB Academy to date, it is important for us to be constantly vigilant and remain fully informed about the issues which affect the local area, city and society in which we teach. Staff are reminded to suspend any 'professional disbelief' that instances of radicalisation 'could not happen here' and to be 'professionally inquisitive' where concerns arise, referring any concerns through the appropriate referral process.

Early intervention is vital and staff must be aware of the established processes for front line professionals to refer concerns about individuals and/or groups. We must have the confidence to challenge, the confidence to intervene and ensure that we have strong safeguarding practices based on the most up-to-date guidance and best practise.

Filtering and Monitoring

To support the prevention of accessing such extremist, radical or inappropriate materials on the Academy ICT Network we have invested in the use of Smoothwall which is the Academy firewall and filtering provision. Smoothwall specialises in the education sector and has a 2 tier checking process as it checks on the Smoothwall network first and then is checks locally on the Academy ICT network. The Academy use Impero which is 3rd party software that combines classroom management, network management, and desktop management in one single consolidated solution.

The two technologies do the following:

- Impero software is available within the ICT department class rooms to be used by the teacher within their lessons
- prevent access to unsuitable sites
- prevent unauthorised use of proxy sites
- enforce acceptable usage policy
- create key word libraries for real-time detection
- determine potential risk through key word glossaries with explanations
- create different policies depending on severity
- capture time stamped screen shots of every violation
- add screenshots to log viewer report
- export violations with details and image to PDF
- evidence misconduct from a centralised log to support disciplinary action
- alert the relevant authority when rules are violated
- log and monitor all web activity
- Impero blocks the users instantly for a period of time dependant on the severity of the violation
- Smoothwall blocks users permanently from accessing the internet if required

The monitoring of any breach by students or staff that occurs due to inappropriate online activity via the filtering system is recorded. As a result, an automated report is compiled and emailed to the safeguarding team daily. The report consists of the user activity which includes:

- username
- date and time stamped
- URL that was accessed
- The reason for it being flagged as a violation

As a result of inappropriate internet or ICT systems use, this will lead to sanctions outlined within the **Academy behaviour policy**.

Curriculum

Our curriculum is “broad and balanced” (Ofsted 2012, April 2014, Sept 2014 and Sept 2015). It promotes respect, tolerance and diversity. Children are encouraged to share their views and recognise that they are entitled to have their own different beliefs which should not be used to influence others.

Our curriculum provision which is underpinned by the SMSC and British values is embedded across the curriculum. It is recognised that children with low aspirations are more vulnerable to radicalisation and therefore we strive to

equip our students with confidence, self-belief, respect and tolerance as well as setting high standards and expectations for themselves.

Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Students are not allowed to access social media sites in the Academy/There are various restrictions on the use of these sites in the Academy that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum, PSHEE and assemblies about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The Academy follows general rules on the use of social media and social networking sites in the Academy:

- Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the Academy's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official Academy blogs created by staff or student's/year groups/Academy clubs as part of the curriculum will be password-protected and run from the Academy website with the approval of a member of staff and will be moderated by a member of staff.
- Students and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The Academy expects all staff and students to remember that they are representing the Academy at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

It is also important to highlight that under S.141F EDUCATION ACT 2002 (ALSO REFERRED TO AS S.13 EDUCATION ACT 2011, If an allegation has been made against a person who is employed or engaged as a teacher at a school and (1) the allegation is that the teacher is or may be guilty of a criminal offence and (2) the allegation is made by or on behalf of a pupil, then it is a criminal offence to publish any information which may lead to the identity of the teacher who is subject to the offence.

Under the Act 'publication' includes any speech, writing, relevant programme or other communication in whatever form, which is addressed to the public at large. Therefore, this includes any allegation which is published in any newspaper or posted on any website including any social network site such as Facebook, Myspace or Twitter, etc. It is important to note that it is not just naming the alleged offender that can amount to an offence; any information published that can lead to members of the public identifying the teacher can be considered an offence and may lead to a criminal conviction. Therefore, a person who publishes the name of a particular school and the age of an alleged offender may find that they have committed a criminal offence, if the information which they publish leads to members of the public being able to identify the teacher.

Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

- they can make students and staff more vulnerable to cyberbullying
- they can be used to access inappropriate internet material

- they can be a distraction in the classroom
- they are valuable items that could be stolen, damaged, or lost
- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The Academy takes certain measures to ensure that mobile phones are used responsibly in the Academy. Some of these are outlined below:

- The Academy will not tolerate cyberbullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school's disciplinary sanctions read the **Academy behaviour policy.**
- Mobile phones can be confiscated by a member of staff, and the device can be searched by a member of the senior leadership team, house team and safeguarding team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.
- Mobile phones must be switched off during lessons or any other formal Academy activities.
- Any student who brings a mobile phone or personal device into the Academy is agreeing that they are responsible for its safety. The Academy will not take responsibility for personal devices that have been lost, stolen, or damaged.
- Images or files should not be sent between mobile phones in the Academy.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

Mobile phone or personal device misuse

Students

- Students who breach Academy policy relating to the use of personal devices will be disciplined in line with the Academy's behaviour policy. Their mobile phone may be confiscated.
- Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

Staff

- Staff are not permitted to take photos or videos of students on personal devices. If photos or videos are being taken as part of the Academy curriculum or for a professional capacity, the Academy equipment will be used.
- The Academy expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours.
- Any breach of Academy policy may result in disciplinary action against that member of staff. More information on this can be found in the **child protection and safeguarding policy**, or in the staff contract of employment.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the Academy. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour policy.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the Academy community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. If an allegation of bullying does come up, the Academy will:

- take it seriously

- act as quickly as possible to establish the facts. It may be necessary to examine Academy systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the Academy will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in the Academy. Repeated bullying may result in a fixed-term or permanent exclusion.

Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The Academy will risk-assess any new technologies before they are allowed in the Academy, and will consider any educational benefits that they might have. The Academy keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Protecting personal data

Ormiston SWB Academy believes that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-Academy and individual progress. The Academy collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the Academy will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the Academy needs. Through effective data management we can monitor a range of Academy provisions and evaluate the wellbeing and academic progression of our Academy body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the Academy will:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the Academy is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our local authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the Academy's safeguards relating to data protection **read the Academy's data protection policy.**

SWB Academy Contacts

Designated Safeguarding Leader	Jane Dickens, Vice Principal	01902 493797
Deputy Designated Safeguarding Leader	Chris Simpson, Safeguarding and Family Support Officer	01902 493797
Deputy Designated Safeguarding Leader	Julie Jones, Student Support Pastoral Leader	01902 493797
Principal	Kerry Inscker	07530 102220
Designated Governor for Child Protection and Academy E-Safety Co-ordinator	Iain Smith, Vice Chair	01902 493797

External Contacts

Centralised Referrals	01902 555392
NSPCC 24-hour Helpline	0808 800 5000
Social Services Emergency Duty Team (out of hours)	01902 555392
Multi-Agency Support Team (MAST)	01902 551974
Wolverhampton Local Children's Safeguarding Board	01902 550477
NSPCC Helpline for Children	0800 1111
NSPCC Help and Advice for Adults	0808 800 5000

Links to Guidance

Government Prevent Strategy -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97976/prevent-strategy-review.pdf
Keeping Children Safe in Education 2016
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf
Ofsted Safeguarding Policy
https://www.gov.uk/government/publications/ofsted-safeguarding-policy