Ormiston Academies Trust

Ormiston Bolingbroke Academy e-Safety & e-Security policy

Policy version control

Policy type	Statutory
Author In consultation with	Les Leese James Miller
Approved by	James Miller, July 2020
Release date	August 2020
Next release date	August 2021
Description of changes	Policy version 1.1: ▪ Dates updated ▪ Minor wording amendments to improve flow and understanding ▪ Amendments made to meet local setting by Liam Hussey, Ormiston Bolingbroke Academy E-Safety Coordinator – October 2020

Contents

1. Introduction

Ormiston Academies Trust (referred to as "the Trust" and any or all of its Academies), understands that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the Trust recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The Trust is committed to providing a safe learning and teaching environment for all pupils and staff and has implemented controls to reduce any harmful risks.

This policy will be updated as necessary to reflect best practice, or amendments made to legislation, and shall be reviewed every 12 months from July 2018.

"E-Safety Coordinator" – member of teaching staff employed at the academy who takes a lead role on e-safety. This person is line managed by the Designated Safeguarding Lead

"Users" – Any person including staff, students or external

"Network Manager" – Senior ICT Technical Lead person

"Staff" – Any person directly employed by the academy

"Pupil" – Any pupil currently registered to the academy

2. Considerations when using the internet

Ormiston Bolingbroke Academy recognises that modern technology is an intrinsic part of modern-day life and our students use ICT extensively both within and outside of education. However, along with the opportunities that ICT offers it also brings with it problems and risks that all staff, students and parents need to be aware of.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk: content: being exposed to illegal, inappropriate or harmful material; contact: being subjected to harmful online interaction with other users; conduct: personal online behaviour that increases the likelihood of, or actually causes harm.

When accessing the internet, individuals are especially vulnerable to several risks which may be physically and emotionally harmful, including:

2.1. Access to illegal, harmful or inappropriate images

2.2. Cyber bullying

2.3. Access to, or loss of, personal information

2.4.   Access to unsuitable online videos or games

2.5.   Loss of personal images

2.6.   Online sexual harassment and abuse

2.7.   Inappropriate communication with others

2.8.   Illegal downloading of files

2.9.   Exposure to explicit or harmful content, e.g. involving radicalisation

2.10.   Plagiarism and copyright infringement

2.11.   Sharing the personal information of others without the individual's consent or knowledge

A detailed overview of e-safety issues as identified and defined by students of Ormiston Bolingbroke

Academy are summarised in Appendix A

3. Roles and responsibilities

3.1.   It is the responsibility of all users to ensure that the internet, is used in an appropriate and legal manner. If any users are witnesses to or believe that ANY illegal or harmful activities have taken, or are taking place, they MUST inform an appropriate member of staff immediately.

3.2.   The network manager is responsible for the implementation and day to day management of the safety systems and software used within the academy and managing any issues that may arise. This includes ensuring that appropriate filtering is in place for all users and that this is up to date.

3.3.   The E-Safety Coordinator will provide technical support and advice to members of staff as required and will support any wider academy CPD.

3.4.   The Principal will ensure there is a system in place which monitors and supports the E-Safety Coordinator, whose role is to work with the Designated Safeguarding Lead (DSL) to carry out the monitoring of e-safety in the academy, keeping in mind data protection requirements.

3.5.   The E-Safety Coordinator will maintain a log of submitted e-safety reports, incidents and technical issues. All incidents and issues will be reported to the Designated Safeguarding Lead (DSL) and the academy Data Protection Lead (DPL) as appropriate.

3.6.   The Academy will ensure that all members of staff are aware of the procedure when reporting e-safety incidents.

3.7.   The E-Safety Coordinator and DSL will carry out regular reviews of internet usage data by all users and address any concerns as they arise. Proactive monitoring MUST take place and the appropriate staff member MUST be alerted directly and automatically of any incidents.

3.8.   Cyber bullying incidents will be reported in accordance with the academy's Anti-Bullying Policy.

3.9. Teachers are responsible for ensuring that e-safety is embedded in the curriculum and safe internet access is always promoted.

3.10. All staff and pupils will ensure they understand and adhere to The Trust's Acceptable Use Policy, which they must sign and return to the Academy. The Academy MUST keep a log of acceptance and this must be updated as changes occur.

3.11. All pupils MUST be made aware of their responsibilities regarding the use of Trust-based ICT systems and equipment, including their expected behaviour.

3.12. All academies MUST meet the minimum requirements of the GDPR ICT Audit or better. If you are unsure or believe that the academy no longer meets this requirement you must inform the DPO immediately.

Detailed responsibilities of staff and other stakeholders of Ormiston Bolingbroke Academy are detailed in Appendix B.

4.eSafety education

4.1. Educating pupils:

4.1.1. The Academy will regularly update pupils to make sure they are aware of the safe use of new technology both inside and outside of the academy.

4.1.2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

4.1.3. Pupils will be taught to acknowledge information they access online, to avoid copyright infringement and/or plagiarism.

4.1.4. Clear guidance on the rules of internet use will be present in all classrooms where ICT is used.

4.1.5. Pupils are instructed to report any suspicious use of the internet and digital devices to a member of staff.

4.1.6. The academy will hold e-safety events, such as Safer Internet Day and Anti Bullying Week, to promote online safety.

4.2. Educating staff:

4.2.1. E-safety training opportunities MUST be available to all staff members, including whole academy activities and CPD accredited training courses where appropriate.

4.2.2. All staff will undergo e-safety training including cyber security on an annual basis to ensure they are aware of current issues and any changes to the provision of e-safety, as well as current developments in social media and the internet.

4.2.3. All staff will undergo an annual "Skills Audit" by the academy that will identify individual CPD needs of staff.

4.2.4. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.2.5. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.2.6. Any new staff are required to undergo online safety and awareness training as part of their induction programme, ensuring they fully understand this policy.

4.2.7. The E-Safety Coordinator will act as the first point of contact for staff requiring general e-safety advice. Safeguarding issues or concerns MUST be processed using the academies Safeguarding processes.

5. Control Measures

5.1. Internet Access

5.1.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with The Trust's Acceptable Use Policy.

5.1.2. A record will be kept by the academy of all pupils who have been granted internet access.

5.1.3. All users in Key Stage 2 and above will be provided with usernames and passwords and must keep these confidential to avoid any other pupils using their login details.

5.1.4. Management systems may be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

5.1.5. Keeping Children Safe in Education compliant filtering systems MUST be in place and in use to reduce any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material. Impero and Smoothwall management systems are in place across the academy network to provide filtering and monitoring of content

5.1.6. Any requests by staff for websites to be added or removed from the filtering list must be authorised by the E-Safety Coordinator and logged.

5.1.7. All Academy systems MUST be protected by up-to-date anti-virus software.

5.1.8. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

5.1.8.1. These accounts MUST be assigned to a single user and logged to ensure that in the event of any abusive, illegal, or behavioral matter can be investigated and allow the investigating office to identify a single individual.

5.1.9. If authorised by the principal, staff can use the internet for lawful and appropriate personal use during out-of-academy hours, as well as break and lunch times. Please Note: All internet activity on academy devices will leave a digital footprint. Any person choosing to use academy devices for personal reasons is giving permission for OAT to have this data until such time that the digital footprint is purged.

5.1.10. Personal use will only be monitored by the network manager, HR or safeguarding staff for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, and would outweigh the need for privacy.

5.1.11. Inappropriate internet access by a member of staff may result in the staff member being restricted.

Ormiston Bolingbroke Academy's approach to filtering and monitoring are detailed in Appendix C

6.Social Networking

6.1. Please note: Additional detail is provided in the Staff AUP. Guidance for staff representing the academy on social media are also directed to the *Expectations around social media accounts for professional purposes* document

6.2. Use of social media on behalf of the academy will be conducted following the processes outlined in The Trust's Social Media Policy.

6.3. Access to social networking sites will be filtered as appropriate.

6.4. Should access be needed to social networking sites for any reason, this will always be monitored and controlled by staff and must be first authorised by the Principal.

6.5. Staff are not permitted to publish comments about the Trust which may affect its reputability.

7. Published content on the academy website and images:

7.1. The Principal will be responsible for the overall content of their academy website and will ensure the content is appropriate and accurate.

7.2. Contact details on the academy website will include the phone number, email and address of the academy.

7.3. Images and full names of pupils, or any content that may easily identify a pupil, must follow the Trust policies relating to the Data Protection Act 2018.

7.4. Pupils are not permitted to take or publish photos of others without permission from the individual and the Academy.

7.5. Staff can take pictures, though they must do so in accordance with academy policies in terms of their sharing and distribution.

7.6. Staff will not take pictures using their personal equipment.

7.7. Any member of staff that is representing the Trust online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the Trust, or any information that may affect its reputability.

8. Mobile devices and hand-held computers:

8.1. The Principal may authorise the use of mobile devices for a pupil and staff where it is seen to be for safety, precautionary or educational use.

8.2. If permitted by the Principal, pupils and staff will access the academy's Bring You Own Device (BYOD) Wi-Fi system using their personal mobile devices and hand-held computers providing the user and/or device meets the academies individual criteria. Internet access will be monitored for any inappropriate use by the network manager when using these devices on the academy network.

8.3. Staff are permitted to use hand-held computers which have been provided by the academy, though internet access will be monitored for any inappropriate use by the network manager and/or DSL.

8.4. Using the academy's devices or network to send inappropriate messages or images is prohibited.

8.5. Personal mobile devices will not be used to take images or videos of pupils or staff.

9. Cyber bullying

9.1. This section must be reviewed alongside the Trust's "Anti-Bullying Policy"

9.2. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive posting of information, images online or direct or indirect messaging.

9.3. The Trust recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that occur.

9.4. The academy will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post.

9.5. The academy will commit to creating a learning and teaching environment which is free from harassment and bullying, for all staff and pupils.

9.6. The Principal will decide whether it is appropriate to notify the police or other appropriate parties regarding any action taken against a pupil or staff member.

10. Reporting misuse

10.1.   The Trust will clearly define what is classed as inappropriate behaviour in the Acceptable Use Policy, ensuring all pupils and staff members are aware of what behaviour is expected of them.

10.2.   Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

10.3.   Appendix D summarizes the multiple methods and procedures for reporting e-safety concerns at Ormiston Bolingbroke Academy

Misuse by pupils:

10.4.   Any instances of misuse should be immediately reported to the E-Safety Coordinator.

10.5.   As a student of Ormiston Bolingbroke Academy, failure to comply with any part of this policy or the Acceptable Use Policy may result in one or more of the following sanctions (in line with behaviour policy) to be faced

   a.   Verbal warning/advice

   b.   Enforced e-safety enrichment

   c.   A ban, temporary or permanent, on the use of the technology facilities.

   d.   A letter/phone call informing parents of the nature and breach of rules.

   e.   A formal interview with parents/carers, the student in question and staff

   f.   Referral to external agencies e.g. police, local authority

   g.   Detention

   h.   Internal exclusion

   i.   Exclusion – fixed term or permanent

   j.   Any other action decided by the Head of Year, E-safety Coordinator, Principal or Governors

10.6.   Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with the "Child Protection and Safeguarding Policy" and reported to the Designated Safeguarding Lead (DSL).

Misuse by staff:

10.7.   Any misuse of the internet by a member of staff should be immediately reported to the Principal.

10.8.   The Principal will deal with such incidents in accordance with the "Allegations of Abuse Against Staff Policy" and may decide to take disciplinary action against the member of staff.

10.9. The Principal will decide whether it is appropriate to notify the police of any action taken against a member of staff.

Use of illegal material:

10.10. In the event that illegal material is found on any of the Trust's networks, or evidence suggests that illegal material has been accessed, the academy must notify the Trust's Head Office for further investigation and support. Where appropriate the police will be contacted.

10.11. If a child protection incident is suspected, the Trust's child protection procedure will be followed – the DSL and Principal will be informed, and the police contacted.

11. Physical Security – Location Access

11.1. All on-site devices which store data MUST be kept in a secure location with appropriate access control for example a server room or hub room. Physical access to the server room must be limited to only those individuals who have legitimate responsibilities to justify such access. If the space is left unattended for ANY period, it MUST be secured before leaving. If keys are used, then the keys MUST not be suited to a master key and MUST be clearly marked "Do Not Duplicate"

11.2. Key allocations must be logged including the date provided. Any losses must also be logged with the appropriate person and key allocations must be fully audited annually.

11.3. Procedures must be in place to ensure access is removed when no longer required. Procedures must also be in place to address lost or stolen keys or access cards. All access to these locations must be audited and must include Names, Time, Date and Reason for access. This log must be kept for a minimum of the last 365 days

11.4. The academy must ensure compliant arrangements are in place for the removal or relocation of any ICT equipment from its normal location. If temporary storage is required for equipment that contains ANY academy data, then the chosen physical location must also meet the security requirements set out above. Note: these requirements relate to data storage only; you must also consider other policies such as health and safety.

12. Data Processing Equipment locations.

12.1. When considering screen locations for data processors the academy MUST consider the ability to be "over seen". If there is any possibility of the data processors screen been "over seen" this issue must be addressed before the device is used to process ANY academy data.

12.2. Users MUST observe the following precautions when using a device to process data, or that has access to any academy data:

12.2.1. Devices are positioned in such a way that information being processed cannot be viewed by person(s) not authorised to view the information. Specific consideration should be given to the location of devices on which high risk information is processed or retrieved and high traffic areas such as reception and other public spaces.

12.2.2. Devices MUST NOT be left logged-on when unattended for ANY period of time.

12.2.3. Accounts MUST NOT be shared with ANY other user for any reason.

12.2.4. Passwords MUST not be shared with any user, including technical staff. Note: Users may be asked to log into a device for technical staff to carry out maintenance or the technical staff may be required to change your password to carry out required work.

12.2.5. Users MUST NOT leave unencrypted or hard copies of "Personal Identifiable" data unattended at any time, including on the academy grounds unless stored in a secure location that meets the physical security statements set out above. NOTE: Unattended data or data access is considered as a Data Breach and MUST BE reported to your local Data Protection Lead (DPL) for investigation by the Data Protection Officer (DPO).

12.2.5.1. For the sake of clarity, the statements above must be adhered to when accessing Academy Data from any device or at any location such as home, public space, friends and family homes, etc. Access to data MUST be secured from other unauthorised users at all times.

13. Inventory

13.1. A requirement of the Trusts building Insurance provider and to meet the obligations of the Data Protection Act 2018 increases the need for securing ICT equipment and as part of the approach OAT is taking, each academy must maintain and keep up to date an audit of ICT equipment.

14. Data Backup

14.1. All data must be backed up to a secure and GDPR Compliant offsite location. Any data that is taken off site or stored offsite for the purpose of back-up must be encrypted to a minimum of 256bit. At no point should all data including all back-up media exist in a single location. Note: "Offsite" is defined as a location that is not geographically located to or have the same environmental concerns as the main academy site.

14.2. Data stored as back-up MUST comply with OAT data retention policy. When data reaches "end of life" all data INCLUDING that stored in ANY backup file in ANY location MUST also be purged.

14.3. A back-up regime MUST allow for any individual piece of data to be recovered in a timely manner. It is accepted that some degree of data loss may occur, but this must not exceed data produced over the last 24 hours.

14.4. The academy MUST conduct back-up testing as set out below (or better):

14.4.1. Daily – Confirm that the last back-up has completed successfully. Rectify any issues as necessary.

14.4.2. Half term – Data integrity check. This can be done by recovering a predefined number of files successfully. This will not require an official test if it has been carried out successfully for a real requirement.

14.4.3. Termly – Disaster Recovery Total loss test

14.5. Users may back-up their data individually, but this back-up must meet the required data security principles in this document.

14.6. The Primary back-ups should be carried out automatically at set intervals and information contained within these back-ups should only be accessible by the ICT Technical Team for verification and restoration. Other back-up methods can be used to allow users direct self-recovery of files in addition to a "Primary Back-up" but all backups must meet the storage and security requirements set out in this document.

14.7. The production environment must not be impacted by the running of back-up jobs. All back-ups must be created, scheduled and run according to the performance and availability requirements of the environment.

15. Malware and Virus Detection and Removal

15.1. Malware (malicious software) and Viruses can infiltrate your systems and software and cause damage or allow your systems to be used for malicious or unlawful activities.

15.2. All academy devices MUST Use Anti-virus / Anti-malware detection and removal software at all times. This software MUST be set to scan on access for all devices and updates as a minimum of monthly. Where possible the software must be configured in such a way to stop unauthorised users from disabling it.

15.3. Users MUST NOT disable any Anti-virus/Anti-Malware software installed on their machine for any reason. If the user has an issue that they believe requires this to happen then they MUST contact a member of the technical team for support.

15.4. Mobile Devices (including academy and personal laptops and mobile phones)

15.5. These devices MUST be encrypted and must be password protected. Encryption level must be equal to or exceed 128bit and the password MUST meet the Password Policy as stated above for laptops. Mobile devices can be secured in several ways but as a minimum MUST have a 4 Digit Pin or better.

15.6. Please note: that device accounts are for an individual's use and must not be shared. If another user requires access to the device this MUST be done using an appropriate account for the users and ensure that the user cannot access any data that they are not officially authorised to access.

15.7. All works devices MUST be encrypted, and password protected. When using mobile phones users must be aware of their surroundings and the ability to be "overheard" when discussing personal identifiable information.

15.8. Any device that is used to access or store academy data including contact information or emails MUST be password and / or 4 Digit PIN protected as a minimum.

15.9. If this device is shared with other people outside of the OAT staff, then the device MUST be set in such a way that the data is not accessible by the other users. As this data is classed as offsite this data MUST be encrypted.

15.10. Mobile Phones and Tablets MUST be kept up to date with Apps and Operating Systems. It is the academy's responsibility to ensure this is carried out for all academy owned devices. Users MUST ensure that their device meets this requirement.

16. Protecting data with passwords

16.1. All accounts MUST be password protected with complexity set to a minimum of:

16.1.1. 8 or more characters
16.1.2. Minimum 1 number
16.1.3. Minimum 1 uppercase

16.2. Passwords must be changed frequently (minimum every 12 months) or immediately if you suspect someone has obtained your password or you believe it may have been compromised.

16.3. Passwords MUST NOT be shared with other users unless the account in questions is a Group Access account.

16.4. All academies MUST carry out an annual password audit. This audit MUST include:

16.4.1. Domain Admin Account including Passwords
16.4.2. Domain User Account and the full name of the person it is allocated too.
16.4.3. Other Domain admin account, what they are used for, who has the account details, password
16.4.4. All hardware accounts (E.g. switches, firewall, etc) full details and password
16.4.5. All external accounts (E.g. Office 365 tenancy, Google-Suite, etc) Account details, password

Please note: No non-technical member of staff is permitted to know any technical management accounts unless signed off by the Principal, this account access must be detailed in the audit including the reason for the access.

Please Note: Audit data MUST be stored a secure manner with limited access and in a way that allows its access to be traced.

17. Patch and Software Updates

17.1. Academies MUST keep all device software and hardware up to date. Please note: Software updates MUST be managed and installed at a site appropriate time, agreed beforehand. For general updates it is recommended that these take place during a significant holiday period to

ensure proper testing can take place prior to deployment and to minimise disruption to the academy. ALL critical updates and patches that are issued by hardware and software vendors MUST be implemented as a matter of urgency.

17.2. It is recommended that academies implement Microsoft Windows Server Update Services (WSUS)

17.3. Please Note: Other software manufacturers have central deployment methods to roll out software, updates and patches. Always check what functionality is available for your products.

Appendix A

Online Safety Issues

Ormiston Bolingbroke Academy recognises that the internet is a fantastic resource that brings endless benefits. However the online world also has problems and risks which we all need to be aware of:

Cyberbullying — when technology is used to hurt other people's feelings without seeing them in person. Cyberbullying can often be more hurtful than face-to-face bullying.

Online Grooming — when strangers try to befriend and take advantage of young people. Often a groomer will aim to meet up with the person they have groomed.

Online Conduct — Everything that you publish and post online creates what is known as your 'Digital Footprint' and stays with you for life. This can affect your reputation and your career.

Radicalisation — when terrorist organisations use the internet to try and encourage young people to become a terrorist or draw young people into extremist activity.

Sexting — when messages and indecent images are sent to/from a young person. This is against the law and can have serious consequences. Sometimes these images can be used in 'revenge porn' acts which is also against the law and can be very upsetting for the victim

Privacy — personal details and information are sometimes hacked into by people with bad intentions,for example bank details to steal a person's money.

Catfishing - pretending to be someone you are not online by posting false information, such as someone else's pictures or name.

Inappropriate Content — there is a lot of content on the internet such as pornography, gambling and violence that is not suitable for young people and should be avoided. Accessing such content may be illegal.

Online Pressure — many people feel pressured online to follow the crowd. This can include getting involved in cyberbullying and using filters to look different. This often has a negative effect on a young person's self-esteem.

Commercialism - Young people's enjoyment online can sometimes be affected by advertising and money making schemes, which can also mean unwillingly spending money online, for example buying points within a game.

Overuse of technology — some young people spend too much time using technology. This often has a negative effect on a person's performance at school, their health and well-being as well as their social life.

Invalid Information — not all the information we see online is true for example 'Fake News' often appears online. You should only ever trust reliable sources.

Copyright and Privacy — work shared online is often protected by copyright law and you may be breaking the law if you use other people's work or download content without permission or without paying for this service.

Online Sexual Harassment and Abuse - Young people may experience harassment, sexual abuse, sexual exploitation or emotional abuse when they use the internet. Children can be at risk of online harassment and abuse from people they know, as well as from strangers. People often feel like there is no escape from online abuse and harassment as abusers can contact them at any time of the day or night.

If you have an e-safety concern or would like more information on the above issues you should speak to any adult in school such as: Mr Hussey - OBA E-safety Co-ordinator, Form tutor, Head of Year / Assistant Head of Year, Mr Easton, Mr Hough, Ms Sothern.

CLICK CEOP Internet Safety

Click on the REPORT TO OBA button on the Academy website

Ormiston Bolingbroke Academy
Nurture • Support • Excellence

Appendix B – E-Safety roles and responsibilities

Role	Key responsibilities
Governors	To ensure that the Academy follows all current e-safety advice to keep the children and staff safe online as part of their responsibilities in relation to safeguarding. To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Link Governor (Sam Crane). To support the Academy in encouraging parents and the wider community to become engaged in e-safety activities.
Principal	Takes overall responsibility for e-safety provision. Take overall responsibility for data and data security (GDPR). To ensure the Academy uses an approved, filtered internet service, which adheres to best practice and recommendations. To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant. To be aware of procedures to be followed in the event of a serious e-safety incident. To receive regular monitoring reports from the e-safety co-ordinator. To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures.
Designated Safeguarding Lead	To line manage the E-Safety Co-ordinator providing advice, support and challenge. To undergo training in E-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from but not limited to; sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming, cyber-bullying. To refer incidents to relevant external organisations. To receive regular monitoring reports from the e-safety co-ordinator.
E-Safety Co-ordinator	Create and audit of e-safety across the Academy, looking at the three key elements of content, conduct and contact. Take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the Academy e-safety policies / documents. Complete a 360 review of current provision to produce an action plan that informs the academy's age appropriate e-safety programme. Promote an awareness and commitment to e-safeguarding throughout the Academy community.

	Maintain and review the e-safety policy. Develop an e-safety log and ensure that it is kept up to date. Liaise with Academy ICT staff / network manager to maintain the safety element of the Academy website and provide a weekly piece for the newsletter. Work with the network manager to ensure that web filtering and wireless networks remain compliant with the Academy's e-safety policy. Provide a half-termly report for SLT and contribute to the Governors' report including an annual presentation to Governors. Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. Continually develop the AUP and ensure it is issued and returned annually. Facilitate training and advice for all staff, including a session in new staff induction, an annual presentation on safety, AUP and social media as well as ensuring in-year starters receive the same presentation and information in a timely manner. Keep updated in e-safety issues and legislation and be aware of the potential for serious child protection issues to arise from: sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming, online bullying and use of social media, extremism and radicalisation.
ICT Curriculum Leader	To oversee the delivery of the e-safety element of the curriculum. To liaise with the e-safety coordinator regularly to facilitate professional discussion around e-safety.
Network Manager / Technicians	To report any e-safety related issues that arise, to the e-safety coordinator. To ensure that users may only access the Academy's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. To ensure that provision exists for misuse detection and malicious attack, e.g. keeping virus protection up to date. To ensure the security of the Academy ICT system. To ensure that access controls / encryption exist to protect personal and sensitive information held on Academy-owned devices. The Academy's policy on web filtering is applied and updated on a regular basis. Keeps up to date with the Academy's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. That the use of the network and email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator.

	To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a critical incident or system failure. To keep up-to-date documentation of the Academy's e-security and technical procedures.
Data Manager	To ensure that all data held is done so in compliance with GDPR guidelines.
Teachers	To embed e-safety issues in all aspects of the curriculum and other Academy activities. To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities/trips). To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	To read, understand and help promote the Academy's e-safety policies and guidance. To read, understand, sign and adhere to the Academy staff Acceptable Use Agreement. To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current Academy policies with regard to these devices. To report any suspected misuse or problem to the e-safety coordinator. To maintain an awareness of current e-safety issues and guidance e.g. Through CPD. To model safe, responsible and professional behaviours in their own use of technology. To ensure that any digital communications with pupils should be on a professional level and only through Academy based systems, never through personal mechanisms, e.g. Email, text, mobile phones, social networking sites, etc.
Pupils	Read, understand, sign and adhere to the Student Acceptable Use Policy. To understand the importance of reporting abuse, misuse or access to inappropriate materials. To know what action to take if they or someone they know feels worried or vulnerable when using online technology. To comply with Academy policy on the use of mobile phones, digital cameras and hand held devices. To understand the importance of adopting good e-safety practice when using digital technologies at all times. To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in Academy and at home. To help the Academy in the creation/ review of e-safety policies.
Parents/carers	To read, understand and promote the Academy Student Acceptable Use Agreement with their children.

	To consult with the Academy if they have any concerns about their children's use of technology. To engage in online activity as a positive role model to their children – ensuring all communication is appropriate.
External users	Any external individual / organisation will accept and acknowledge the Acceptable Use Policy prior to using any equipment or the internet within Academy.
E-safety group	Members of the E-Safety Group will assist the E-Safety Coordinator with the production / review / monitoring of the Academy E-Safety policy / documents. Act as a 'critical friend' to the e-safety co-ordinator. Provide a wide range of opinions in terms of age and experience from the whole Academy community. Monitor the impact of e-safety education and to identify and fill any gaps. Manage initiatives such as anti-bullying week and Safer Internet Day. Be creative in considering the Academy response to developing e-safety issues.

Appendix C: Filtering and Monitoring at Ormiston Bolingbroke Academy

Ormiston Bolingbroke Academy is proud to invest time and money in filtering and monitoring at to keep students and staff safe. The two core pieces of software for this are Impero Education Pro and Smoothwall.

Impero EdProtect's inbuilt keyword libraries are a core part of its e-safety software offering. The libraries have been carefully developed in conjunction with a number of charities and specialist organisations. All terms are assigned severity ratings designed to help staff respond appropriately and within context of a student's wider behaviour, both online and offline. The keyword libraries are built using Unicode, supporting multiple languages, and the academy also adds localised terms as and when required.

Library categories include but are not limited to:

- Adult content

- Bullying and trolling

- Counter-radicalisation (including Arabic script)

- Drugs and substance misuse

- Eating disorders

- Grooming

- Illegal content

- LGBT derogatory language

- Race and religious hatred

- Self-harm

- Sexting

- Suicide

- Weapons and violence

On a half termly basis, the e-safety co-ordinator will ask a mixture of students and staff to undertake some keyword tests on the network. These will be using key terms that would be expected to be blocked in school and would trigger an alert. Key terms to be used will be agreed in advance with the Principal. This audit will be closely monitored and relevant action taken should any content not be blocked or not trigger an alert.

Smoothwall provides security to the Academy network and is used for; virus prevention, firewall services, certificate authentication, screening and also acts as second line of web filtering in addition to Impero.

Response:

Impero Education Pro monitors the school network and when a keyword is detected, whether in an application, typed in an email, on social media, in a search engine, present on a website or in a URL, the incident is captured. This capture is timestamped and logged with a screenshot, or video clip, to provide 'who, what, where' style information, putting the incident into context. Severe alerts are sent via email directly to the e-safety co-ordinator and for immediate attention. Moderate and minor captures are stored in the capture log and are dealt with on a daily basis. Captures are triaged and dealt with on a case by case basis.

A complete log of all online activity, including screenshot and video captures to evidence misuse or potential risk, provides a historical timeline of user activity, including username, computer name, application or website, time, date and screenshot/video recording evidence can be accessed by the e-safety co-ordinator. The capture management log, with incident handling and reporting tools, provides recorded evidence of identified risk which can be shared with safeguarding staff, parents/carers or external agencies as and when required.

Captures and other evidence of misuse may be dealt with by the e-safety co-ordinator, escalated to the safeguarding team, the relevant year team(s) or Senior Leadership Team, or deescalated as a 'false positive'. The flow chart below represents this process
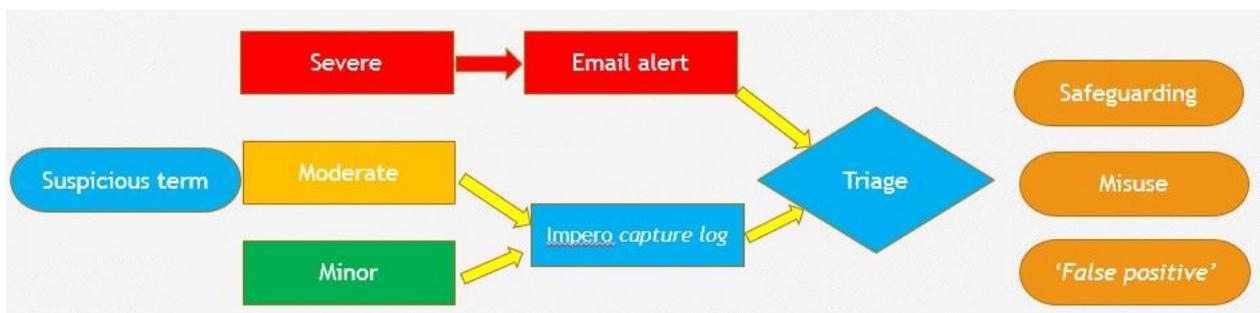
Appendix D – Reporting routes

```
                          ┌─────────────────────┐
                          │   E-Safety Concern   │
                          └─────────────────────┘
      ┌──────────────┬──────────┴──────────┬──────────────┐
      │              │                     │              │
┌───────────┐ ┌─────────────┐ ┌─────────────┐ ┌───────────┐ ┌───────────┐
│ E-Safety  │ │ Safeguarding│ │ Report to   │ │  Email:   │ │   CEOP    │
│Coordinator│ │ Team:       │ │ OBA         │ │Safeguarding│ │  report   │
│ Mr Hussey │ │ Mr Easton,  │ │ anonymously │ │@ob-       │ │  button   │
│           │ │ Mrs Ryan,   │ │ on school   │ │ac.co.uk   │ │           │
│           │ │ Ms Sothern  │ │ website     │ │           │ │           │
└───────────┘ └─────────────┘ └─────────────┘ └───────────┘ └───────────┘
                                     │
                              ┌─────────────┐
                              │    Issue    │
                              │ investigated│
                              └─────────────┘
                                     │
                              ┌─────────────┐
                              │ Intervention│
                              │ as per      │
                              │ relevant    │
                              │ policy/     │
                              │ policies    │
                              └─────────────┘
                                     │
                              ┌─────────────┐
                              │Issue resolved,│
                              │logged and   │
                              │shared with  │
                              │relevant     │
                              │partners as  │
                              │necessary    │
                              └─────────────┘
```