Rye College Policy

Policy Title:	Online Safety
Leadership Responsibility:	Designated Safeguarding Lead
Review Body:	Executive Headteacher
Date:	February 2021
Review:	February 2022

Context

Rye College recognises the importance of treating online safety as an ever-present serious safeguarding issue. It is important to protect and educate both students and colleagues with supportive mechanisms, policies and protocols to protect and support the community.

Ofsted reviews online safety measures in schools and there are numerous Acts of Parliament (**Appendix A**) which can be used to safeguard both students and colleagues in academies. The safeguarding aspects of online safety are evident in all our ICT and safeguarding policies and procedures throughout the academy, and it is essential this constantly developing area of technology is kept under review.

This policy links all the ICT, safeguarding and other policies and procedures to reflect how the academy deals with online safety issues. The documents referred to in this online safety policy have been developed by various groups including:

- Advisory Councils in other Academies;
- Headteachers, Leaders, Designated Safeguarding Leads;
- ICT Subject Leaders and IT technical support;
- Teachers and associate colleagues;
- Parents and families;
- Students.

Relevant policies

This policy operates in conjunction with the following academy policies:

- Accessibility;
- Anti-bullying;
- Attendance;
- Behaviour Management;
- Child Protection and Safeguarding;
- CCTV;
- Complaints;
- Curriculum;
- Data Protection;
- Health and Safety Procedures;
- Lettings;
- Loan of Equipment;

- Lost Property and Liability;
- Records Management;
- Screening, Searching and Confiscation;
- Special Educational Needs and Disabilities (SEND);
- Technical Security;
- Trust Data Protection;
- Trust Employee Code of Conduct (Handbook);
- Trust Health and Safety;
- Trust Safeguarding.

Objectives

This policy applies to all members of the college community (including colleagues, students, volunteers, families, visitors, community users) who have access to and are users of our technology systems, both in and out of the college.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off-site and empowers colleagues 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 academy, but is linked to membership of the academy.

The Education Act 2011 increased these powers with regard to 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 Management Policy**.

The academy 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

Executive Headteacher/Headteacher/Head of School

The Executive Headteacher/Headteacher/Head of School is responsible for the online safety policy and for reviewing the effectiveness of the policy including:

- Regular meetings with the Online Safety Officer;
- Attendance to Online Safety Group meetings;
- Regular monitoring of online safety incident logs;
- Regular monitoring of filtering/change control logs;
- Reporting to relevant committee meetings.

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the college community, though the day-to-day responsibility for online safety will be delegated to the **Online Safety Lead**.

The Headteacher and senior leaders are aware of the procedures to be followed in the event of a serious online safety allegation being made against a colleague.

The Headteacher and senior leaders are responsible for ensuring the Online Safety Lead and other relevant colleagues receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and senior leaders will ensure there is a system in place to allow for monitoring and support of those who carry out internal online safety monitoring. This is to provide a safety net and also support those colleagues who take on important monitoring roles. The trust undertakes quality assurance through the work of the Compliance Officer.

Senior leaders receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

As the Designated Safeguarding Lead, **Miss Carpenter** is also the **Online Safety Lead**.

The Online Safety Lead:

- Leads the Online Safety Group;
- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the **Online Safety Policy**;
- Ensures all colleagues 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 colleagues;
- Liaises with the Local Authority, Trust or relevant body;
- Liaises with academy IT Support;
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments;
- Reports to relevant meetings of the Advisory Council to discuss current issues, review incident logs and filtering/change control logs;
- Reports regularly to senior leaders.

Network Manager

Those with technical responsibilities:

- Ensure technical infrastructure is secure and is not open to misuse or malicious attack;
- Ensure the academy meets required online safety technical requirements, and complies with any Local Authority, Trust or other relevant body's Online Safety Policy;
- Ensure users may only access networks and devices through properly enforced password protection;
- Ensure a filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person;
- 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 (see **Technical Security Policy**);
- Ensure the use of the networks, internet and digital technologies are regularly monitored so any misuse or attempted misuse can be reported to the Headteacher or senior leaders and the Online Safety Lead for investigation;
- Ensure monitoring systems are implemented and updated as outlined in relevant policies.

Teachers and Associate Colleagues

Colleagues must:

- Ensure they have an up-to-date awareness of online safety matters and of the current Online Safety Policy and practice;
- Ensure they have read, understood, signed or routinely agree to the relevant Acceptable Use Agreement (**Appendix C**);
- Ensure they report any suspected misuse or problem to the Headteacher, senior leaders or Online Safety Lead for investigation;
- Ensure all digital communications with students and families are professional and only carried out using official systems;
- Embed online safety issues in all aspects of the curriculum and other activities;
- Ensure students understand and follow the Online Safety Policy and Acceptable Use Agreement;
- Ensure students have a good understanding of digital research skills and the need to avoid plagiarism and uphold copyright regulations;
- Ensure they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other activities (where allowed) and implement current policies regarding these devices;
- Guide students to sites, in lessons where internet use is pre-planned, checked as suitable for their use and secure processes for dealing with any unsuitable material found in internet searches.

Designated Safeguarding Lead

Miss Carpenter is the Designated Safeguarding Lead.

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection and safeguarding issues to arise from:

- Sharing of personal data;
- Access to illegal or inappropriate materials;
- Inappropriate online contact with adults or strangers;
- Potential or actual incidents of grooming;
- Online bullying.

It is important to emphasise these are **safeguarding issues**, not **technical issues**.

Online Safety Group

The Online Safety Group provides a consultative forum that has wide representation from the college community, with responsibility for issues of online safety and the monitoring the Online Safety Policy including the impact of initiatives.

Members of the online safety group include the Designated Safeguarding Lead, Communication Officer, Life Education Co-ordinator and members of IT Support. The group is working towards student and parent representatives.

This group will assist with the development of online safety education and digital safeguarding across the college. It ensures colleagues and students are kept up-to-date with an ever-changing

digital world via the Friday Briefing and Life Education curriculum. It provides information for families via the website.

Members of the Online Safety Group assist the Online Safety Lead to:

- Produce, review and monitor the Online Safety Policy;
- Produce, review and monitor filtering and requests for filtering changes;
- Map and review the online safety curriculum provision – ensuring relevance, breadth and progression;
- Monitor network, internet, filtering, incident logs;
- Consult stakeholders – including parents and students about online safety provision;
- Monitor improvement actions identified through review.

Students

Our young people:

- Are responsible for using our digital technology systems in line with the 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;
- Are 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 or use of images and on online bullying;
- Should understand the importance of adopting good online safety practices when using digital technologies out of school and realise the Online Safety Policy covers their actions out of school, if related to their membership of the college community.

While regulation and technical solutions are very important, their use is balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of our online safety provision. Online safety education is provided by:

- A planned online safety programme provided as part of Computing, PSHE and other lessons – this will include both the use of ICT and new technologies inside and outside the academy;
- Key online safety messages reinforced as part of a planned programme of assemblies and tutorial activities;
- Students taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information;
- Students helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT, internet and mobile devices both inside and outside the academy;
- Students taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet;
- Rules for use of ICT systems and internet posted in relevant rooms.

Families

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

- Digital and video images taken at college events;
- Access the academy's www.office.com and online student records;
- Their child's personal devices in the academy (where permitted).

Parents are responsible for endorsing the relevant Acceptable Use Agreement.

Research shows many parents do not fully understand the issues and are less experienced in the use of ICT than their children. The academy will therefore take every opportunity to help parents understand these issues through:

- Parents' evenings;
- Newsletters;
- Letters;
- Website;
- Information about all relevant national or local online safety campaigns and literature;
- Information about useful organisations or support services for reporting online safety issues (see **Appendix B**).

Community users

Community users who access academy systems or programmes as part of wider academy provision will be required to comply with the relevant Acceptable Use Agreement before being provided with access to our systems.

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 and digital literacy is therefore an essential part of the academy's online safety provision. Young people need the help and support of the academy to recognise and avoid online safety risks and build their resilience.

In planning our online safety curriculum, the academy will refer to:

- DFE Teaching Online Safety in Schools;
- Education for a Connected Word Framework;
- SWGfL Project Evolve – online safety curriculum programme and resources.

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

- A planned online safety curriculum provided as part of Computing, PHSE and other lessons;
- Key online safety messages reinforced as part of a planned programme of assemblies and tutorial activities;
- Students taught in all lessons to be critically aware of the materials and content they access online and guided to validate the accuracy of information;
- Students taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Students 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 helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside academy;
- Colleagues 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 processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where students are allowed to freely search the internet, colleagues 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, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, colleagues can request **IT Support** to 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 and approved by the **Online Safety Lead**.

Education – Families

Many families 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 and regulation of 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 academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities;
- Letters, newsletters, web site, learning platform (www.office.com);
- Parents information sessions;
- High profile events and campaigns e.g. Safer Internet Day;
- Reference to the relevant web sites/publications:
    - www.saferinternet.org.uk;
    - www.childnet.com/parents-and-carers;
    - See **Appendix B** for further materials.

Education –Wider Community

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

- Family learning courses in use of new digital technologies, digital literacy and online safety;
- Online safety messages targeted towards grandparents and the extended family;
- Academy website providing online safety information for the wider community;
- Sharing online safety expertise and good practice with other local schools;
- Supporting community groups e.g. Early Years Settings, Childminders, youth, sports or voluntary groups to enhance their online safety provision.

Education and training – Colleagues and volunteers

It is essential all colleagues receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to colleagues. This will be regularly updated and reinforced. An audit of the online safety training needs of all colleagues will be carried out regularly;
- All new colleagues should receive online safety training as part of their induction programme, ensuring they fully understand the online safety policy and acceptable use agreements;
- It is expected some colleagues will identify online safety as a training need within the performance management process;
- Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;
- Online Safety Policy and its updates will be presented to and discussed by colleagues in meetings and training sessions;
- Online Safety Lead will provide advice, guidance and training to individuals as required.

Technical – infrastructure, equipment, filtering and monitoring

The academy is responsible for ensuring the infrastructure and network is as safe and secure as is reasonably possible and policies and procedures approved within this policy are implemented. The academy also ensures the relevant people named in the above sections are effective in carrying out their online safety responsibilities:

- Academy technical systems managed in ways that ensure the academy meets recommended technical requirements;
- Regular reviews and audits of the safety and security of academy technical systems;
- Servers, wireless systems and cabling must be securely located and physical access restricted;
- All users will have clearly defined access rights to academy technical systems and devices;
- All users will be provided with a username and secure password by **IT Support** who keep an up to date record of users and their usernames. Users are responsible for the security of their username and password;
- The "administrator" passwords for academy systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (See **Technical Security Policy**);

- The **Network Manager**, working with the **Business Manager**, is responsible for ensuring software licence logs are accurate and up to date and 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. There is a clear process in place to deal with requests for filtering changes;
- Internet filtering and monitoring should ensure children are safe from terrorist and extremist material when accessing the internet;
- The academy has provided enhanced or differentiated user-level filtering;
- IT Support 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. This academy uses Smoothwall;
- A system is in place (via My Concern and /or Spiceworks) for users to report any actual or potential technical incident or 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 devices are protected by up to date virus software;
- An agreed procedure is in place for the provision of temporary access of "guests" onto the school systems: by agreement with the Headteacher, **IT Support** can provide temporary access to trainee teachers, supply teachers, volunteers and visitors;
- An agreed procedure is in place regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school: All school devices should only be used by the individual to which the devices is issued for purposes directly relating to the academy (e.g. work or education);
- An agreed procedure is in place regarding the use of removable media by users on academy devices: the academy does not allow use of removable media e.g. memory sticks/CDs/DVDs;
- Colleagues are forbidden from downloading executable files and installing programmes on academy devices;
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies including 'Bring Your Own Device' (BYOD)

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

The absolute key to considering the use of mobile technologies is that students, colleagues and wider academy community understand the primary purpose of having their personal device at school is educational and that this is irrespective of whether the device is school-owned or personally-owned. Teaching about the safe and appropriate use of mobile technologies should be included in the online safety education programme.

Potential Benefits of Mobile Technologies

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and communities of interest. By effectively maximising the use of such resources, schools not only have the opportunity to deepen student learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high-tech world in which they will live, learn and work.

The Acceptable Use Agreements consider the use of mobile technologies.

Our academy allows:

	Academy devices			Personal devices		
	Academy owned and allocated to a single user	**Academy owned for use by multiple users**	**Authorised device[1]**	**Student owned**	**Colleague owned**	**Visitor owned**
Allowed in school	Yes	Yes	Yes	Yes[2]	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet access only	No	No	No	No	Yes	No
No network access	No	No	No	Yes	No	Yes

- The academy has provided technical solutions for the safe use of mobile technology for academy devices and personal devices:
    - All academy devices are controlled though the use of Mobile Device Management software;
    - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access);
    - The academy has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices;
    - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted;
    - Appropriate exit processes are implemented for devices no longer used at an academy location or by an authorised user; (These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.)
    - All academy devices are subject to routine monitoring;

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

[2] The academy should add below any specific requirements about the use of personal devices in the school/academy e.g. storing in a secure location, use during the day, liability, taking images etc

- Pro-active monitoring has been implemented to monitor activity.

- When personal devices are permitted:
  - All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access;
  - Personal devices are brought into the academy entirely at the risk of the owner and the decision to bring the device in to the academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school;
  - The academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home);
  - The academy accepts no responsibility for any malfunction of a device due to changes made to the device while on the academy network or whilst resolving any connectivity issues;
  - The academy recommends that devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security;
  - The academy is not responsible for the day-to-day maintenance or upkeep of the user's personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.
- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
  - Devices may not be used in tests or exams;
  - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements;
  - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network;
  - Users are responsible for charging their own devices and for protecting and looking after their devices while in the academy;
  - Personal devices should be charged before being brought to the academy as the charging of personal devices is not permitted during the school day;
  - Devices must be in silent mode while onsite;
  - Academy devices are provided to support learning. It is expected students will bring devices to the academy as required;
  - Confiscation and searching (England) - the school/academy has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate;
  - The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work are not permitted;
  - The software/apps originally installed by the academy must remain on the academy owned device in usable condition and be easily accessible at all times. From time to time the academy may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure users have not removed required apps;

- The academy will ensure devices contain the necessary apps for school work. Apps added by the academy will remain the property of the academy and will not be accessible to students on authorised devices once they leave the academy roll. Any apps bought by the user on their own account will remain theirs;
- Users should be mindful of the age limits for app purchases and their usage, and should ensure they read the terms and conditions before use;
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately;
- Devices may be used in lessons in accordance with teacher direction;
- Colleague-owned devices should not be used for personal purposes during teaching sessions;
- Printing from personal devices will not be possible.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing colleagues and students instant use of images that they have recorded themselves or downloaded from the internet. However, colleagues, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying 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:

- When using digital images, colleagues should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- Written permissions from parents or carers will be obtained before photographs of students are published on the school website/social media/local press;
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). 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/carers comment on any activities involving other *students* in the digital images;
- Only permitted colleagues and volunteers are allowed to take digital images to support educational aims, and must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of colleagues should not be used for such purposes.
  In Rye College, only the following colleagues and volunteers are permitted to take photographs on academy equipment for use beyond the classroom:
  - **Communications Officer**;
- Care should be taken when taking digital images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy 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/pupils 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;
- Student's work can only be published with the permission of the student and parents or carers.

Communications

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

	Colleagues and other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected colleagues	Not allowed	Allowed	Allowed at certain times	Allowed with permission	Not allowed
Mobile phones may be brought onsite	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	X						X	
Use of personal email addresses in academy, or on academy network	X							X
Use of academy email for personal emails				X				X
Use of messaging apps		X						X
Use of social media		X						X
Use of blogs		X						X

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

- The official academy email may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Colleagues and students should therefore use only the academy email service to communicate with others when in school, or on academy systems (e.g. by remote access);
- Users must immediately report, to the nominated person – in accordance with the academy 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 colleagues and students or parents/carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications;
- 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 academy website and only official email addresses should be used to identify colleagues.

Social Media - Protecting Professional Identity

All schools, trusts and local authorities have a duty of care to provide a safe learning environment for students and colleagues. Schools, trusts and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Colleagues who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *academy, trust* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, colleagues 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.

Colleagues should ensure:

- No reference should be made in social media to students, families or colleagues;
- 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 *academy, trust* or local authority;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

- Approval by the Headteacher;
- Clear processes for administration and monitoring the accounts – involving at least two colleagues;
- Systems for reporting and dealing with abuse and misuse;
- Understanding that incidents may be dealt with under academy disciplinary procedures.

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear the colleague is not communicating on behalf of the academy 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 academy 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 academy. The academy will effectively respond to social media comments made by others according to a defined policy or process. The academy's use of social media for professional purposes will be checked regularly by the **Communications Officer** and **Online Safety Group** to ensure compliance with academy policies.

Dealing with unsuitable or inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. online-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 an academy context, either because of the age of the users or the nature of those activities.

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

		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,	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

proposals or comments that contain or relate to:	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	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices; • Creating or propagating computer viruses or other harmful files; • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords); • Disable/Impair/Disrupt network functionality through the use of computers/devices; • Using penetration testing equipment (without relevant permission). **Illegal activities will be reported to the Police.**						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
Online gaming (educational)			X			
Online gaming (non-educational)					X	
Online gambling						X
Online shopping/commerce				X		
File sharing					X	
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. YouTube				X		

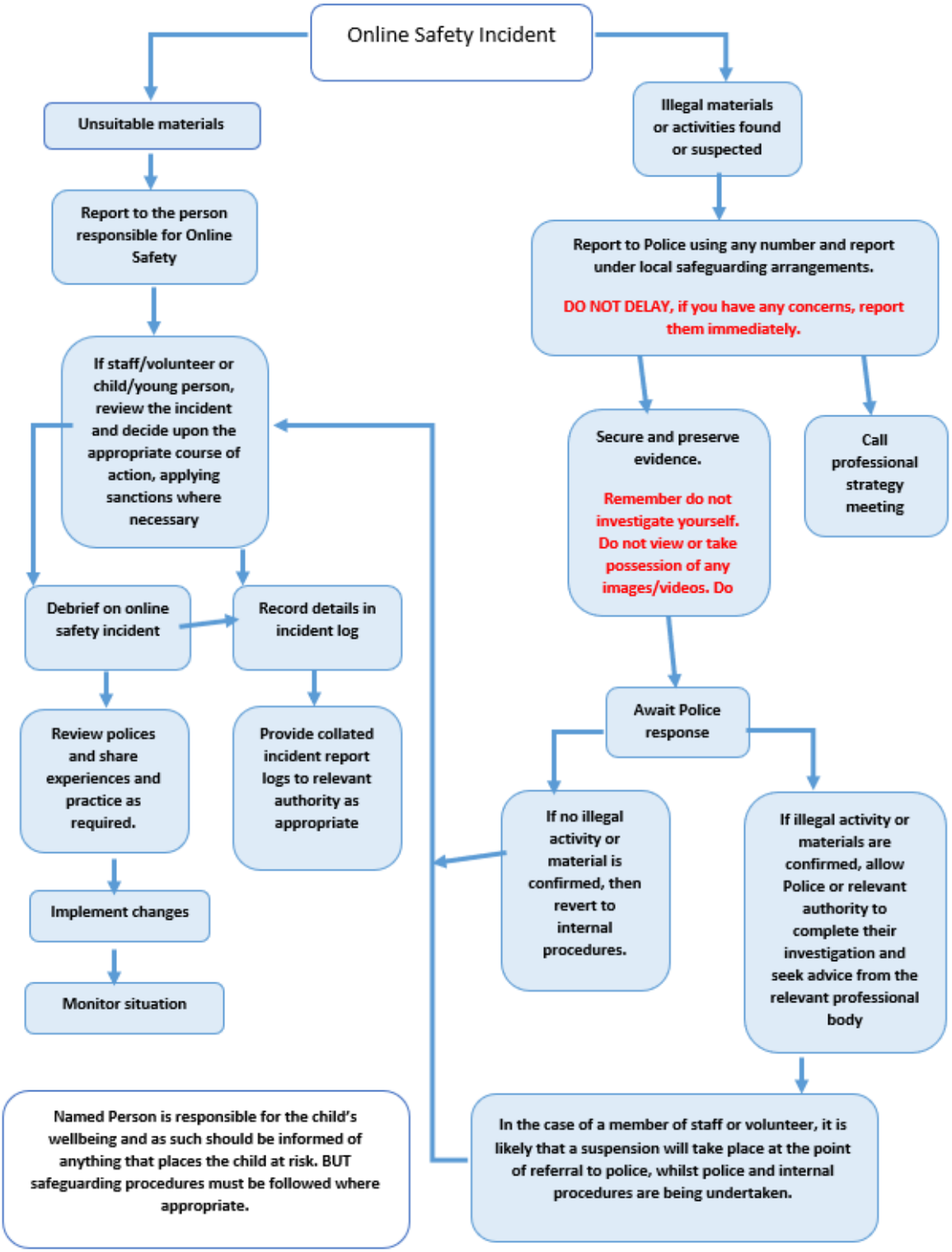
Responding to incidents of misuse

This guidance is intended for use when colleagues 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 the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the Online Safety Incident Flowchart for responding to such incidents and report immediately to the Police.

Online Safety Incident Flowchart



Other Incidents

It is hoped all members of the academy community will be responsible users of digital technologies, who understand and follow academy 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 leader 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 the relevant colleagues should have appropriate internet access to conduct the procedure, but also 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 Local Authority/Trust 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 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;
- Offences under the Computer Misuse Act (see User Actions above);
- 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 all of the above steps are taken as they will provide an evidence trail for the academy and possibly the Police and demonstrate visits to these sites were carried out for safeguarding purposes. The information should be retained by the group for evidence and reference purposes.

Academy actions and sanctions

It is more likely the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important any incidents are dealt with as soon as possible in a proportionate manner, and members of the school community are aware incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal Behaviour Management Policy and disciplinary procedures as follows:

	Potential Actions/Sanctions								
Student Incidents	Refer to class teacher/tutor	Refer to Curriculum Leader / Student Hub	Refer to Headteacher	Refer to Police	Refer to IT Support for action e.g. filtering	Inform parents/carers	Removal of network 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							X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X							X	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	X							X	
Unauthorised downloading or uploading of files					X				X
Allowing others to access academy network by sharing username and passwords					X		X		
Attempting to access or accessing the academy network, using another student's/pupil's account					X				X
Attempting to access or accessing the academy network, using the account of a member of staff					X		X		X
Corrupting or destroying the data of other users					X				X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X		X	X		X
Continued infringements of the above, following previous warnings or sanctions		X		X		X	X		X
Actions which could bring the academy 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/academy's filtering system	X				X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident					X	X	X		X
Deliberately accessing or trying to access offensive or pornographic material		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		

	Potential Actions/Sanctions							
Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Human Resources	Refer to Compliance Officer	Refer to LADO	Refer to Police	Refer to Technical Support	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	X	X		X
Inappropriate personal use of the internet/social media/personal email	X	X	X		X			X
Unauthorised downloading or uploading of files	X	X	X				X	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			X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X		X			X	X
Deliberate actions to breach data protection or network security rules	X	X		X			X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	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
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		X	X		X	X		X
Actions which could compromise the staff member's professional standing	X	X	X		X			X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X					X
Using proxy sites or other means to subvert the school's/academy's filtering system		X		X			X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X				X	X
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X
Breaching copyright or licensing regulations		X		X		X		X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X		X

Monitoring and reviewing

The academy will monitor the impact of the policy using:

- Logs of reported incidents;
- Monitoring logs of internet activity (i.e. ISP, academy network or managed service as appropriate);
- Internal monitoring data for network activity;
- Surveys/questionnaires of students, parents/carers and colleagues.

The policy will be reviewed by the Executive Headteacher and Advisory Council annually, or more regularly, in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to online safety as advised by the online safety committee or others.

January 2021 BBL

EQUALITIES

We recognise that our students bring with them a wide variety of behaviours influenced by life experiences outside college. We aim to respond to each case professionally, objectively and compassionately. We are sensitive when working with children and families with specific needs and experiences and we continuously seek ways to promote successful partnerships. The basis of differentiation will vary dependant on the needs of each case but we will consider the views of parents and families, colleagues and external agencies together with any Statement of Special Educational Need or Education, Health and Care Plan. We will also ensure compliance with the Trust's Equality Policy considering students with protected characteristics and making reasonable adjustments for students with a disability within the meaning of the Equality Act 2010. Both the college and Trust respects the Public Sector Equality Duty (PSED) that requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different people when carrying out their activities. By following the Trust's Equality Policy, the college seeks to eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by such legislation.

DATA PROTECTION

Rye College [The Academy] processes personal data in accordance with the data protection principles embodied in the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Academy complies with the requirements of the data protection legislation as detailed in the Trust Data Protection Policy.

All colleagues are aware of the principles of data protection and will not process personal data unless necessary. The Academy safeguards the personal data it collects through the operation of the Trust's data protection policy and processes and the IT policy. In addition, the Academy has taken steps to ensure that all its contracts that process data have the GDPR compliant provisions.

Appendix A: Acts of Parliament Relevant to online safety in Academies

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment. (This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.)

Computer Misuse Act 1990 (sections 1–3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (e.g. using someone else's password to access files).
- Gain unauthorised access, as above, to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (e.g. caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgment. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)

It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years imprisonment.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and data users must comply with important data protection principles when handling personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for academies which relate to cyber-bullying/bullying:

- Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of students off-site.
- Academy staff member can confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the academy behaviour/anti-bullying policy.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false, or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Obscene Publications Act 1959 and 1964

Publishing an 'obscene' article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows, or ought to know, that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Public Order Act 1986 (sections 17–29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (e.g. to ensure communications are relevant to academy activity or to investigate or detect unauthorised use of the network.) Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as 'sexting'). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Typically, teachers, social workers, health professionals, connexions staff etc. fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Appendix B: Useful services for reporting online safety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

Online content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Media content inappropriate for children

If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through *ParentPort* at www.parentport.org.uk. Click on 'Make a Complaint' and ParentPort will take you straight to the right place to complain to.

Scams

If you have been 'scammed, ripped off or conned' you can report to *Action Fraud* on 0300 123 2040 or www.actionfraud.police.uk. This service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

Getting help/advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.
- Cybermentors: For bullying issues, go online and talk to other children to get help and support www.cybermentors.org.uk. Cybermentors is run by Beatbullying.
- Youth 2 Youth: A young persons' helpline which offers confidential peer support via telephone, email and online chat – www.youth2youth.co.uk.
- Get Connected: A free confidential helpline for young people, open 1pm-11pm every day. Tel 0808 8084994.

Getting help/advice: for parents

- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk.
- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 8pm, on 08451 205204 www.kidscape.org.uk.
- *Childnet International* Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young

people to deal with them'. Contact details are: www.childnet.com, phone 020 7639 6967, email info@childnet.com.

Getting help/advice: for professionals working with children

- *Professionals' online safety helpline*: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with online safety issues. The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0844 3814772 (calls on this number are charged at the local rate).

Appendix C: Acceptable Use Agreements

By using the school's ICT network and hardware, the user agrees to abide by the Acceptable Use Agreement.

i. Acceptable Use Agreement (Summary for College ICT Systems)

By accepting, you agree to the terms outlined.

I will only use College ICT systems approved for my use e.g. computers, laptops and tablets.

I will only use email accounts approved for my use e.g. ryecollege.co.uk.

I will not use personal emails to send and receive personal data or information.

I will not use, share or store personal data relating to students or staff members for non-school related activities.

I will not use, share or store personal data with students, staff members or third parties unless approved to do so by the Network Manager/Headteacher.

I will only use removable media approved by the Network Manager.

I will secure all school-related information stored on any removable media in line with the GDPR.

I will delete any chain letters, spam and other emails from unknown sources without opening them.

I will only access learning materials from sources approved by the Network Manager/Headteacher.

I will only access the internet for personal use outside school hours which includes break and lunch.

I will not search for, view, download, upload or transmit any explicit, inappropriate or illegal material when using the internet.

I will not use College ICT systems to access, download, upload, send, receive, view or display any of the following material:

- Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school;
- Content relating to a person's protected characteristics such as sexual orientation, gender assignment, religion, race, disability or age;
- Online gambling;
- Content which may adversely affect the reputation of any organisation, including the school and trust, or person, whether they are known to be true or false;
- Any sexually explicit content;
- Any other illegal content;
- Any personal data or information.

I will not share school-related passwords unless approval has been given by the Network Manager.

I will not install any software onto College ICT systems unless approved by the Network Manager.

[Students] will only use the College ICT systems to:

- Complete homework and coursework, and to prepare for lessons and exams;
- Undertake revision and research;
- Gather or process information for school-related or extra-curricular activities.

[Colleagues] will use, share and store personal data in line with the GDPR using encryption, where appropriate.

Reporting misuse

I will report any misuse or breaches of this agreement to the Network Manager/Headteacher.

I understand my internet use is monitored and recognise any breach of the Acceptable Use Agreement will be managed under the appropriate disciplinary policy.

I will adhere to the **Online Safety Policy** and Acceptable Use Agreements in full.

ii. Technology acceptable use agreement – Students

Rye College understands the benefits technology can have on enhancing the curriculum and students' learning; however, we must ensure students respect college property and use technology appropriately.

To achieve this, we have created this acceptable use agreement which outlines our expectations of students when using technology, whether this is on personal or college devices, and on or off the premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined.

Using technology in school

I will only use ICT systems, e.g. computers, laptops and tablets, which my classroom teacher has given me permission to use.

I will only use the approved email account that has been provided to me by the IT technician.

I will not store or use any personal data relating to a student or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my classroom teacher.

I will delete any chain letters, spam, and other emails from unknown senders without opening them.

I will ensure that I get permission from my classroom teacher before accessing learning materials, e.g. source documents, from unapproved sources.

I will only use the internet for personal use during out-of-school hours, including break and lunchtimes. During school hours, I will use the internet for school work only.

I will not share my passwords, e.g. to my school email address, with anyone.

I will not install any software onto school ICT systems unless instructed to do so by my classroom teacher.

I will adhere to the e-safety guidelines I have been taught.

I will only use the school's ICT facilities to:

- Complete homework and coursework, and to prepare for lessons and exams.
- Undertake revision and research.
- Gather or process information for extra-curricular activities, e.g. creating the school newsletter.

I will not use the school's ICT facilities to access, download, upload, send, receive, view or display any of the following:

- Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school;
- Content relating to a person's protected characteristics such as sexual orientation, gender assignment, religion, race, disability or age;
- Online gambling;
- Content which may adversely affect the reputation of any organisation, including the school and trust, or person, whether they are known to be true or false;
- Any sexually explicit content;
- Any other illegal content;
- Any personal data or information.

Mobile devices

I will use school-owned mobile devices, e.g. laptops and tablets, for educational purposes only.

I will only use personal mobile devices during out-of-school hours and in accordance with the Behaviour Management Policy.

I will ensure my mobile device is either switched off or set to silent mode during school hours, and will only use my device to make or receive calls when my classroom teacher permits me to do so.

I will seek permission from my classroom teacher before a school-owned mobile device is used to take images or recordings.

I will not use any mobile devices to take pictures of fellow students unless I have their consent and the consent of a member of staff.

I will not use any mobile devices to send inappropriate messages, images or recordings.

I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

I will not access the WiFi system using personal mobile devices.

I will not take or store images or videos of staff members on any mobile device, regardless of whether it is school-owned.

Social media

I will not use any school-owned mobile devices to access personal social networking platforms.

I will not communicate or attempt to communicate with any staff members over personal social or gaming networking platforms.

I will not accept or send 'friend requests' from/to any staff members over personal social or gaming networking platforms.

I will ensure that I apply the necessary privacy settings to any social networking sites.

I will not publish any comments or posts about the school on any social networking platforms which may affect the school's reputation.

I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.

I will not post any material online that:

- Is offensive;
- Is private or sensitive;
- Infringes copyright laws;
- Damages the school's reputation;
- Is an image or video of any staff, parent or nonconsenting student.

Reporting misuse

I will ensure that I report any misuse or breaches of this agreement by students or staff members to the headteacher.

I understand that my use of the internet will be monitored by the Online Safety Lead and recognise the consequences if I breach the terms of this agreement, e.g. having personal devices confiscated.

I understand that the headteacher may decide to take disciplinary action against me in accordance with the school's Behavioural Management Policy if I breach this agreement.

I acknowledge that I have read and understood this agreement, and ensure that I will abide by each principle.

iii. Technology acceptable use agreement – Colleagues

Whilst Rye College promotes the use of technology, and understands the positive effects it can have on enhancing students' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Using technology in school

I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.

I will only use the approved email accounts that have been provided to me.

I will not use personal emails to send and receive personal data or information.

I will not share sensitive personal data with any other students, staff or third parties unless explicit consent has been received.

I will ensure that any personal data is stored in line with the GDPR.

I will delete any chain letters, spam and other emails from unknown sources without opening them.

I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.

I will only use the internet for personal use during out-of-school hours, including break and lunch times.

I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.

I will not share school-related passwords with students, staff or third parties unless permission has been given for me to do so.

I will not install any software onto school ICT systems unless instructed to do so by the Network Manager or Headteacher.

I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis.

I will only use recommended removable media and will keep this securely stored in line with the GDPR.

I will only store data on removable media or other technological devices that has been encrypted of pseudonymised (this involves replacing / removing names or other identifiers which are easily attributed to individuals).

I will only store sensitive personal data where it is necessary and which is encrypted.

I will provide removable media to the e-safety officer for safe disposal once I am finished with it.

Mobile devices

I will only use school-owned mobile devices for educational purposes.

I will only use personal mobile devices during out-of-school hours, including break and lunch times.

I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.

I will ensure mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.

I will not use mobile devices to take images or videos of students or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.

I will not use mobile devices to send inappropriate messages, images or recordings.

I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

I will not access the WiFi system using personal mobile devices, unless permission has been given by the headteacher or Online safety lead.

I will not use personal and school-owned mobile devices to communicate with students or parents.

I will not store any images or videos of students, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.

In line with the above, I will only process images or videos of students, staff or parents for the activities for which consent has been sought.

I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised (this involves replacing / removing names or other identifiers which are easily attributed to individuals) and give permission for the Online Safety Lead to erase and wipe data off my device if it is lost or as part of exit procedures.

Social media and online professionalism

If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.

I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the headteacher before accessing the site.

I will not communicate with students or parents over personal social or gaming networking sites.

I will not accept 'friend requests' from any students or parents over personal social or gaming networking sites.

I will ensure that I apply the necessary privacy settings to any social or gaming networking sites.

I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.

I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of students, staff or parents, on any online website.

I will not post or upload any images and videos of students, staff or parents on any online website without consent from the individual(s) in the images or videos.

In line with the above, I will only post images or videos of students, staff or parents for the activities for which consent has been sought.

I will not give my home address, phone number, mobile number, social or gaming networking details or email addresses to students or parents – any contact with parents will be done through authorised school contact channels.

Working at home

I will adhere to the principles of the GDPR when taking work home.

I will ensure I obtain permission from the headteacher and data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.

I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised (this involves replacing / removing names or other identifiers which are easily attributed to individuals).

I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.

I will ensure my personal device has been assessed for security by the DPO and Online Safety Lead before it is used for lone-working.

I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.

I will act in accordance with the school's **Technical Security Policy** when transporting school equipment and data.

Training

I will ensure I participate in any online training offered to me, and will remain up-to-date with current developments in social media and the internet.

I will ensure that I allow the Online Safety Lead and DPO to undertake regular audits to identify any areas of need I may have in relation to training.

I will ensure I employ methods of good practice and act as a role model for students when using the internet and other digital devices.

I will ensure that I deliver any training to students as required.

Reporting misuse

I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online safety Policy, e.g. to monitor students' internet usage.

I will ensure that I report any misuse by students, or by staff members breaching the procedures outlined in this agreement, to the headteacher.

I understand that my use of the internet will be monitored by the e-safety officer and recognise the consequences if I breach the terms of this agreement.

I understand that the headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.