Wye School
The best in everyone™
Part of United Learning

Online Safety Policy

Review Timetable

The Policy will be reviewed every two years, as set out below:	
Policy reviewed centrally	n/a
Policy tailored by individual schools	September 2025
Policy ratified by Local Governing Bodies	October 2025
Renewal Date	October 2027
Author	Luke Magee & Riona Sparks

1. Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	September 2023
The implementation of this online safety policy will be monitored by the:	Riona Sparks DSL
Monitoring will take place at regular intervals:	Annually
The online safety policy will be reviewed biannually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2027
Should serious online safety incidents take place, the following external persons/agencies should be informed as necessary:	Local Area Safeguarding Officer Claire Ledger TEL: 03000 418707 / 07917 602 413 EMAIL: claire.ledger@theeducationpeople.org United Learning DSL Frazer Smith Frazer.smith@unitedlearning.org.uk If a crime has been committed contact the Police on 101 or online. https://www.police.uk/pu/contact-the-police/report-a-crime-incident/

The school will monitor the impact of the policy using:

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

- staff

2. **Scope of the Policy**

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

The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix 1 for the link to the act). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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

3. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety (e-safety) of students, staff, volunteers, and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

4. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so. The policy also considers the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

5. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

5.1 The Local Governing Body (LGB)

The LGB has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet

The governor who oversees online safety is Margaret Williams and is responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy.

This will be carried out by the LGB receiving regular information from the DSL about safeguarding issues including online safety. A member of the LGB has taken on the role of Safeguarding Governor and this role includes oversight of E-Safety, being kept informed of any E-Safety issues and how they are dealt with by the school Safeguarding Team.

5.2 The Principal and Senior Leadership Team

- The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead who is the DSL.
- The Principal should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and should refer to the Safeguarding policy.
- The Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

5.3 The designated safeguarding lead

Details of the roles of the school's DSL/DDSLs are set out in Annex C of Keeping Children Safe in Education (DfE).

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Keeping the Principal and/or governing board informed of any online safety trends or issues

This list is not intended to be exhaustive.

5.4 The ICT manager

The ICT manager function at Wye School is shared between the United Learning central IT team and the school-based IT technician and they are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy (this would normally be a function of the pastoral team, with technical support from the IT team);

This list is not intended to be exhaustive.

5.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that students follow the school's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;

This list is not intended to be exhaustive.

5.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet usage as set out in the Parent/Carer Handbook.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

5.7 Visitors and members of the community

Visitors and members of the community who access school systems or programmes or use the school's ICT systems or internet as part of the wider school provision will be made aware of this policy (when relevant) and will be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use and sign a Community User AUA before being provided with access to school systems.

5.8 Students

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

6. Education/Training

6.1 Educating Students

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

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

- A planned online safety curriculum should be provided as part of Computing and PHSE lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities

We follow the National Curriculum computing programmes of study.

Under the new requirement, **all** schools have to teach:

- Relationships and sex education and health education in secondary schools

This new requirement includes aspects about online safety:

*By the **end of secondary school**, students will know:*

- *Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g., pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared, and used online*
- *How to identify harmful behaviours online (including bullying, abuse, or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.

6.2 Educating Parents/Carers

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

The school will therefore seek to provide information and awareness of internet safety to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions

- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Head of Year, who will involve the DSL if there are any safeguarding concerns.

Concerns or queries about this policy can be raised with the Principal.

6.3 Educating and training staff/volunteers

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

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations).
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

6.4 Educating and training LGB

Members of the LGB should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding.

This may be offered in several ways:

- Attendance at training provided by the Local Authority/United Learning/National Governors Association/or other relevant organisation

7. Protecting children from online abuse

Taken from the NSPCC "Protecting children from online abuse" (23.12.2020)

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

Children and young people can be revictimised (experience further abuse) when abusive content is recorded, uploaded, or shared by others online. This could happen if the original abuse happened online or offline.

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

7.1 Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school anti-bullying policy.)

7.2 Emotional Abuse

Emotional abuse is emotional maltreatment of a child, which has a severe and persistent negative effect on the child's emotional development (Department for Education, 20171; Department of Health, 20172; Scottish Government, 20143; Wales Safeguarding Procedures Project Board, 20194). It's also known as psychological abuse.

Most forms of abuse include an emotional element, but emotional abuse can also happen on its own.

Children can be emotionally abused by anyone:

- parents or carers
- family members
- other adults
- other children

Online examples of emotional abuse can include (but are not limited to):

- verbal humiliation

- name-calling
- constant criticism
- restricting social interaction
- exploiting or corrupting
- encouraging a child to take part in criminal activities
- forcing a child to take part in activities that are not appropriate for their stage of development
- terrorising
- threatening violence
- bullying
- deliberately frightening a child
- deliberately putting a child in a dangerous situation

7.3 Consensual and non-consensual sharing of nudes and semi-nude images and or videos (also known as sexting or youth produced sexual imagery);

This is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Children and young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

If a child or young person originally shares the image consensually, they have no control over how other people might use it.

If the image is shared around peer groups, it may lead to bullying and isolation. Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child (anyone under the age of 18), even if the person doing it is a child. If reported to the police, they will make a record but may decide not to take any formal action against a young person.

7.4 Sexual abuse

Child sexual abuse (CSA) is when a child is forced or persuaded to take part in sexual activities. This may involve physical contact or non-contact activities and can happen online or offline (Department for Education, 2018; Department of Health, Social Services and Public Safety, 2017; Scottish

Government, 2014; Wales Safeguarding Procedures Project Board, 2019). Children and young people may not always understand that they are being sexually abused.

Contact abuse involves activities where an abuser makes physical contact with a child. It includes:

- sexual touching of any part of the body, whether the child is wearing clothes or not
- forcing or encouraging a child to take part in sexual activity
- making a child take their clothes off or touch someone else's genitals
- rape or penetration by putting an object or body part inside a child's mouth, vagina or anus.

Non-contact abuse involves activities where there is no physical contact. It includes:

- flashing at a child
- encouraging or forcing a child to watch or hear sexual acts
- not taking proper measures to prevent a child being exposed to sexual activities by others
- making a child masturbate while others watch
- persuading a child to make, view or distribute child abuse images (such as performing sexual acts over the internet, sexting or showing pornography to a child)
- making, viewing or distributing child abuse images
- allowing someone else to make, view or distribute child abuse images
- meeting a child following grooming with the intent of abusing them (even if abuse did not take place)
- sexually exploiting a child for money, power or status (child sexual exploitation).

7.5 Child Sexual Exploitation

Child sexual exploitation (CSE) is a type of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (Department for Education, 2017; NIdirect, 2018; Scottish Government, 2018; Wales Safeguarding Procedures Project Board, 2019).

Children and young people in sexually exploitative situations and relationships are persuaded or forced to perform sexual activities or have sexual activities performed on them in return for gifts, drugs, money or affection.

CSE can take place in person, online, or using a combination of both.

Perpetrators of CSE use a power imbalance to exploit children and young people. This may arise from a range of factors including:

- age
- gender
- sexual identity
- cognitive ability
- physical strength
- status
- access to economic or other resources (Department of Education, 2017).

Sexual exploitation is a hidden crime. Young people have often been groomed into trusting their abuser and may not understand that they're being abused. They may depend on their abuser and be too scared to tell anyone what's happening because they don't want to get them in trouble or risk losing them. They may be tricked into believing they're in a loving, consensual relationship.

When sexual exploitation happens online, young people may be persuaded or forced to:

- have sexual conversations by text or online
- send or post sexually explicit images of themselves
- take part in sexual activities via a webcam or smartphone (Hamilton-Giachritsis et al, 2017).

Abusers may threaten to send images, video, or copies of conversations to the young person's friends and family unless they take part in further sexual activity. Images or videos may continue to be shared long after the sexual abuse has stopped.

7.6 Radicalisation

Information taken from: https://www.getsafeonline.org/social-networking/online-radicalisation/

Radicalisation by extremist groups or individuals can be perpetrated via several means: face-to-face by peers, in organised groups in the community and, increasingly, online. Their targets are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

However, extremists attempt to influence vulnerable people, the internet invariably plays some kind of role … being widely used both to create initial interest, and as reinforcement to other means of communication. As is the case with everything it is used for, the internet enables considerably larger numbers of people to be reached, in a wider geographic area, and with less effort by the perpetrators.

The power of social media is well-known, and it is this that is the main channel for such grooming – be it Facebook, Twitter, Snapchat, Tic Toc or the multitude of other sites and apps. Other online channels include chatrooms, forums, instant messages, and texts. All are also used by extremists for their day-to-day communication, as is the dark web.

Social media is also used for research by extremists, making it easy for them to identify those who may be vulnerable from what they reveal in their profiles, posts/tweets, photos, and friend lists.

7.7 The school's response to online abuse

To help prevent online abuse we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss examples of online abuse with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover examples of online abuse. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on examples of online abuse its impact and ways to support students, as part of safeguarding training.

In relation to a specific incident of online abuse, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

8. Mobile Technologies (including BYOD/BYOT)

Wye School does not routinely allow students to use their own devices at school. There may be exceptions for health and SEN reasons, these will be negotiated with parents and a clear agreement made as to what is acceptable use at school, which will be communicated to the student and monitored. There may be occasions where devices are used such as to take photographs for GCSE portfolios, where a child has a device, and no activity will require a child to have a device.

9. Use of digital and video images

On joining Wye School all parents are asked to consent, or deny consent, for the use of images of their children by the school and outside agencies. Consent status is recorded on Arbor and should be consulted before any images are taken, displayed or shared. The United Learning copyright policy applies to images once taken:

10. Data Protection

When sharing information staff will ensure they comply with group data protection policies and keep records of disclosures as required by these policies.

11. Technical – infrastructure/equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to school technical systems and devices.**
- **All users will be provided with a username and secure password** by IT support, who will keep an up-to-date record of users and their usernames. **Users are responsible for the security of their username and password**.
- The "master/administrator" passwords for the school systems, used by the Network Manager (or other person) must also be available to the Head/Principal or other nominated senior leader and kept in a secure place (e.g., school safe)
- The ICT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- **Internet access is filtered for all users.** The School uses rocket light speed software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated, and internet use is logged and regularly monitored. The e-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Principal. There is a clear process in place to deal with requests for filtering changes. If a member of staff requires a website to be unblocked, they must contact IT support.
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.** N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students/students etc)
- school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. Staff contact IT support detailing the nature of the breach or incident.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, 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. The school uses ESET protect on all school computers.

- An agreed policy is in place for the provision of temporary access of "guests" (e.g., trainee teachers, supply teachers, visitors) onto the school systems. Guests sign the acceptable usage policy before being given access to the school computers.
- An agreed policy is in place regarding the extent of personal use that users (staff/students/students/community users) and their family members are allowed on school devices that may be used out of school. Students using devices at home sign the Wye School equipment loan form.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices. Only staff with administrative access can download executable files or install programmes.
- An agreed policy is in place (acceptable usage policy) regarding the use of removable media (e.g., memory sticks/CDs/DVDs) by users on school devices. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**. Staff sign and agree to the acceptable usage policy, (please see appendix 2)

12. How the school will respond to issues of misuse

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

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

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

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

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

Specific student/staff misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Appendix 1 - References, further reading and useful links

The Education Act 2011
https://www.legislation.gov.uk/ukpga/2011/21/contents

The Education and Inspections Act 2006
https://www.legislation.gov.uk/ukpga/2006/40/contents

GOV.UK (30.6.2020), 'Guidance: Education for a Connected World', Available at: https://www.gov.uk/government/publications/education-for-a-connected-world

LGfL (2021), 'Online Safety and Safeguarding', Available at: https://www.lgfl.net/online-safety/default.aspx

National Online Safety (2021), 'Online Safety Education for the Whole School Community', Available at: https://nationalonlinesafety.com/

NSPCC Learning 23.12.2020), 'Protecting children from online abuse', Available at: https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse

The Key (23.12.2020), 'Online safety policy: models and examples', Available at: https://schoolleaders.thekeysupport.com/policy-expert/pastoral/online-safety-policy-model-examples/#section-0

United Learning (2021), 'Policies Portal', Available at: https://hub.unitedlearning.org.uk/sites/policies

Appendix 2 – Acceptable Use Policy-Staff Agreement

United Learning ICT Acceptable Use Policy

Adopted by the Finance & Infrastructure Committee, July 2015

All employees must read and agree to abide by this Acceptable Use Policy before they can be allowed to use devices or services provided by or on behalf of United Learning. By completing the relevant section of the Annual Renewal form you agree to the following:

a. An authorized representative of the Group may view, with just reason and without notice or notification, any communications you send or receive material you store on the Group's computers/ services or logs of websites you have visited. This data, regardless of where hosted, belongs to United Learning at all times. It is the Group's policy not to view colleagues' emails without good cause.
b. You will only access those services/ aspects of services which you have been given permission to use.
c. You will not use United Learning resources to operate your own business.
d. You will not attempt to remove any of the security measures put in place by United Learning to ensure the integrity of its services, the security of its data or the appropriateness of employee activity.
e. Any communication from a United Learning related account (email, social media) or account which identifies you as belonging to United Learning will be appropriate in tone and content.
f. You will exercise caution when sending information via email to ensure that it is addressed to the correct recipient(s) and is the correct information (particularly when attaching documents). Personal data (that by which an individual could be identified) must not be transferred to other recipients unless encrypted or password protected, in line with the requirements of Data Protection legislation.
g. You will not transfer United Learning data outside of the organisation's systems except via Group email or encrypted media. This includes the use of cloud storage and personal email accounts. *For example, saving files to Dropbox or emailing them to a personal Hotmail account may resolve logistical problems you are having but run the risk of those data leaving United Learning's control.*
h. You will use the Internet and other services for appropriate activity only. United Learning considers inappropriate activities to include gambling (outside of workplace Lottery syndicates), pornography and sites promoting views which run counter to the organisation's ethos.

i. You will not share your access credentials with anyone. Delegated access to calendars/ email should be granted to administrative support staff, where required.

j. You will not download, use, distribute or otherwise communicate any material which, in so doing, infringes copyright.

k. The use of language deemed aggressive, offensive, or intimidating is not acceptable. You must not write anything on a website or send by email or other medium anything which could be reasonably be deemed offensive.

l. Use of a personal device to access any United Learning data is permitted, subject to the acceptance of the separate Bring Your Own Device policy.

m. Breach of this policy may result in disciplinary action.

Appendix 3 – Acceptable Use Policy-Parent/Student Agreement

Wye School Internet and Email Use Agreement
(Note: All Internet and email activity is subject to monitoring)
The Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet to enhance their learning and provide facilities for research, collaboration, and communication. You will be aware that the Internet is host to a great many illegal and inappropriate websites, and as such we will ensure as far as possible that your child is unable to access such sites. We can do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child. The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child, we will inform you of the circumstances. At the beginning of each school year, we explain the importance of internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety; we also inform them that we can monitor their activity. All children are given the opportunity to ask questions and give their viewpoint.

By enrolling your son/daughter at Wye School, you are agreeing that:

-I have read the above and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network.
-I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

As a student I will:

-only use the school ICT for schoolwork that the teacher has asked me to do.
-not to look for or show other people things that may be upsetting.
-show respect for the work that other people have done.

-not use other people's work or pictures without permission to do so.
-not damage the ICT equipment; if I accidentally damage something, I will tell my teacher.
-not share my password with anybody. If I forget my password, I will let my teacher know.
-not use other people's usernames or passwords.
-not share personal information online with anyone.
-not download anything from the Internet unless my teacher has asked me to.
-let my teacher know if anybody asks me for personal information.
-let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
-be respectful to everybody online; I will treat everybody the way that I want to be treated.
-understand that some people on the Internet are not who they say they are, and some people can be unpleasant.
-I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
-I understand that if I break the rules in this charter there will be consequences of my actions and my parents will be told.