




<b>Formally adopted by the Governing Board/ Trust of:-</b>	<b>Corvus Education Trust</b>
<b>On:-</b>	18 <sup>th</sup> May 2020
<b>Chair of Governors/Trustees:-</b>	David Jessup 
<b>Date for Review:-</b>	Summer 2021

## Online Safety Policy

### Introduction

The Online Safety Policy is part of the schools Safeguarding policy and relates to other policies including those for behaviour, personal, social and health education (PSHE) and for citizenship. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

The Trust has an appointed online safety lead (Mrs Anderson) who has been CEOP trained.

Our Online Safety Policy has been written by the school, building on the NCC Online Safety Policy and government guidance. It has been agreed by the senior management, staff and approved by trustees. The Online Safety Policy and its implementation will be reviewed annually.

It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. This Policy document is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

### Scope of the Policy

This policy applies to all members of the Corvus Education community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Corvus Education digital technology systems, both in and out of the school buildings. The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the Corvus Education 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 Corvus Academy schools but is linked to membership of.

Corvus Education 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.

**The purpose of this policy is to:**

- Set out the key principles expected of all members of the school community with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

## ***Roles and Responsibilities***

### **Trustees/Governors**

Corvus Education are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Trustees receiving regular information about online safety incidents and monitoring reports. It also has two appointed online safety Trustees – Chris Nicholls and David Jessup. The role of the Online Safety Trustee will include:

- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors meetings

### **Headteacher/Principal and Senior Leaders**

- The Executive Headteacher 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.
- The Executive Headteacher and the Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Executive Headteacher and SMT 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 Executive Headteacher 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.

### **Online Safety Lead**

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority and MAT
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets with Online Safety Trustee to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Trustees and Governors as necessary
- reports regularly to SMT as necessary

### **Network Manager/Technical staff**

Those with technical responsibilities are responsible for ensuring:

- that Corvus Education's technical infrastructure is secure and is not open to misuse or malicious attack
- that Corvus Education meets required online safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Principal and SMT; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in Corvus Education policies

### **Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Corvus Education online safety policy and practices
- they have read, understood and signed the staff ICT Code of Conduct.
- they report any suspected misuse or problem to the Executive Headteacher, member of SMT or Online Safety Lead for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies

- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

### **Designated Safeguarding Lead**

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

### **Pupils:**

- are responsible for using the Corvus Education digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations – age appropriate
- 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 – age appropriate
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Corvus Education online safety policy covers their actions out of school, if related to their membership of the school

### **Parents/carers**

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

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in the school (where this is allowed)

## **Our whole school approach to the safe use of ICT**

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities
- Online safety teaching is embedded into the school curriculum and schemes of work

## **The main areas of risk for our school community can be summarised as follows:**

### **Content**

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

### **Contact**

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

### **Conduct**

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

## **Communication**

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and in the staffroom on the Safeguarding wall
- Policy to be part of school induction pack for new staff, including information and guidance where appropriate
- All staff must read and sign the 'Staff Code of Conduct' before using any school technology resource
- Regular updates and training on online safety for all staff, including any revisions to the policy
- Acceptable Use Policy will be discussed with staff and pupils at the start of each year. It will be issued to whole school community, on entry to the school.

## **Handling Concerns**

- The school will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE)
- Staff and pupils are given information about infringements in use and possible sanctions.
- Designated Safeguarding Lead (DSL) acts as first point of contact for any safeguarding incident whether involving technologies or not
- Any concern about staff misuse is always referred directly to the Executive Headteacher, unless the concern is about the Headteacher in which case the concern is referred to the Chair of Governors

## **Education and Curriculum**

### **Pupil online safety curriculum**

Our Schools:

- have a clear, progressive online safety education programme as part of the Computing Curriculum. This covers a range of skills and behaviours appropriate to their age and experience
- will remind students about their responsibilities through the pupil Acceptable Use Policy
- ensure staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright
- ensure that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights – age appropriate

### **Staff and governor training**

Our Schools:

- make regular up to date training available to staff on online safety issues and the school's online safety education program

### **Parent/Carer awareness and training**

Our Schools:

- provide information for parents/carers for online safety on the school website
- run a rolling programme of online safety advice, guidance and training for parents

## **Incident management**

In our schools:

- there is strict monitoring and application of the online safety policy, including the Staff ICT code of conduct and the Acceptable Use Policy. There is a differentiated and appropriate range of sanctions

- support is actively sought from other agencies as needed (i.e. the local authority, [UK Safer Internet Centre helpline](#), [CEOP](#), Police, [Internet Watch Foundation](#)) in dealing with online safety issues
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

## **Managing IT and Communication System**

### **Internet access, security and filtering**

In our schools:

- we follow guidelines issued by the Department for Education to ensure that we comply with minimum requirements for filtered broadband provision

#### **School Internet provision**

- The school uses a 100% Prevent Duty compliant Internet Service Provider.

#### **Content filter**

- The Internet Service Provider uses a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and highly effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.
- Filtering is applied on various levels according to age appropriate material. Pupils have strictly filtered categories and staff have a more relaxed filtering policy to allow them to teach. A default level of pupil level filtering is applied even if guests or unknown users access the connection.
- Internet access is monitored and a report is available to identify any breaches or to provide an audit trail.
- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

#### **Portable storage media**

Staff are not allowed to use their own portable media storage (USB Keys etc).

If staff use USB sticks they should be encrypted, have passwords and be provided by the school.

#### **Security and virus protection**

The school subscribes to an Antivirus software program.

The software is monitored and updated regularly by the school technical staff

Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICT Technician.

## **Personal use of the Internet and ICT resources**

Some equipment (including laptops) is available for loan to staff, with permission from the Headteacher.

All staff must sign the ICT code of conduct. Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment must adhere to all aspects of this Online Safety Policy. School equipment must not be utilised for personal use.

## **E-mail**

### **Our schools**

- Provide staff with an email account for their professional use (Office 365 account) and makes clear personal email should be through a separate account
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

Pupils email:

- We use school provisioned pupil email accounts that can be audited
- Pupils are taught about the online safety and 'etiquette' of using e-mail both in school and at home.
- Pupils email through Office 365 or on the schools VLE platform DB Primary

Staff email:

- Staff will use LA or school provisioned e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

### **School website**

- The school web site complies with statutory DfE requirements
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

## **Equipment and Digital Content**

See Mobile phone and camera image Policy.



## **Digital images and video**

In our schools:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs
- Staff sign the school's ICT Code of Conduct

## **Use of the Internet and ICT resources by school staff**

### **E Safety policy and training**

All staff will be given the School Online Safety Policy and its importance explained annually as part of safeguarding training updates. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils. In order to safeguard all stakeholders, the use of mobile phones is restricted. Mobile phones **will not** be used for filming or photography.

### **The Internet**

The Internet provides a wealth of resources, teaching materials and information that teachers can use across the curriculum. It allows staff to share resources with other schools, and to engage in debate and discussion. We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning. To enable staff to make full use of these important resources, the Internet is available in school to all staff for professional use.

## **ICT Equipment and Resources**

The school also offers staff access to appropriate ICT equipment and resources, including computers, laptops, tablets, interactive whiteboards, data projectors, digital cameras, video camcorders, sound recorders, control and data logging equipment and a range of professional and curriculum software.

### **Professional use**

Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home.

Staff are also careful to consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Equal Opportunities policy.

Staff who need support or INSET in using ICT as part of their professional practice are encouraged to ask for support from the Computing subject leader or Executive Headteacher.

## **Use of the Internet and ICT resources by pupils**

### **Online Safety for Pupils**

We believe it is our responsibility to prepare pupils for their lives in the modern world and ICT is an integral part of that world. At our school we are committed to teaching pupils to use the ICT effectively and appropriately in all aspects of their education.

## **Internet access at school**

### **Use of the Internet by pupils**

Internet access is carefully controlled by teachers according to the age and experience of the pupils and the learning objectives being addressed. Pupils are always actively supervised by an adult when using the Internet and computers with Internet access are carefully located so that screens can be seen at all times by all who pass by.

### **Using the Internet for learning**

The Internet is now an invaluable resource for learning for all our pupils. We use it across the curriculum both for researching information and a source of digital learning materials.

Using the Internet for learning is a part of the Computing Curriculum (Sept 2014)

We teach all of our pupils how to find appropriate information on the Internet and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

- Teachers carefully plan all Internet-based teaching to ensure that pupils are focussed and using appropriate and relevant materials.
- Children are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary.
- They are taught how to recognise the difference between commercial and non-commercial web sites, and how to investigate the possible authors of web-based materials.
- They are taught that web-based resources have similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them.

### **Teaching safe use of the Internet and ICT**

We think it is crucial to teach pupils how to use the Internet safely, both at school and at home, and we use the CEOP Thinkuknow safety code and program and encourage the children to use this with their parents at home. <https://www.thinkuknow.co.uk/>

### **Suitable material**

We encourage pupils to see the Internet as a rich and useful resource, but we also recognise that it can be difficult to navigate and find appropriate material. Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before suggesting them to children, or using them in teaching.

### **Non-Education materials**

As well as Internet material directly related to the curriculum, we encourage children to visit appropriate entertainment and child-oriented activity sites that have interesting and relevant activities, games and information, in school and at home.

There is a selection of links to such resources available from on the school website, on our VLEs and some links might be sent home as homework.

### **Unsuitable material**

Despite the Internet being filtered, occasionally pupils may come across something that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken. They are told to switch off the monitor or screen.

The action will include:

1. Making a note of the website and any other websites linked to it.
2. Informing the ICT Technician and the LA.
3. Discussion with the pupil about the incident, and how to avoid similar experiences in future.
4. Teacher to log incident.

### **Cyberbullying - Online bullying and harassment**

Online bullying and harassment via Instant messaging, mobile phone texting, e-mail and chat rooms are potential problems that can have a serious effect on pupils.

Pupils are taught how to use the Internet safely and responsibly, mainly using the CEOP Thinkuknow program. There is no access to public chat-rooms, Instant Messaging services and bulletin boards in school.

We encourage pupils to discuss any concerns or worries they have about online bullying and harassment with staff, and have a range of materials available to support pupils and their families.

- Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with school child protection procedures.

### **Contact details and privacy**

Pupils are taught that sharing this information with others can be dangerous. Pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.

### **Deliberate misuse of the Internet facilities**

Pupils have discussed the rules for using the Internet safely and appropriately.

Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse. Sanctions will include:

#### **Unsuitable material** (e.g. online games, music downloads etc)

- \_ Initial warning from class teacher
- \_ Report to Headteacher
- \_ Letter to parent/carer

#### **Offensive material** (e.g. pornographic images, racist, sexist or hate website or images etc)

- \_ Incident logged and reported to Head teacher
- \_ Initial letter to parent/carer
- \_ Removal of Internet privileges/username etc
- \_ Meeting with Parent/Carer to re-sign Internet use agreement
- \_ Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

### **Protecting personal data**

Personal data will be recorded, processed, transferred, and made available according to the current GDPR ACT 2018.

## **Education – 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.

Corvus Education will therefore seek to provide information and awareness 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
- Parents/carers are reminded about social networking risks and protocols through our parental Acceptable Use Policy and additional communications materials when required.

## **Education – The Wider Community**

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

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The Corvus Education websites will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools

## **Social networking**

### **Social Media - Protecting Professional Identity**

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

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

School staff should ensure that:

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

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

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

**Personal Use:**

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the Corvus Education or impacts on the MAT, it must be made clear that the member of staff is not communicating on behalf of the MAT with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon Corvus Education 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

**Dealing with unsuitable/inappropriate activities**

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

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on,	<p>Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978</p> <p>N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – <a href="#">UKSIC Responding to and managing sexting incidents</a> and <a href="#">UKCIS – Sexting in schools and colleges</a></p>					X

material, remarks, proposals or comments that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						
<ul style="list-style-type: none"> <li>Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>Creating or propagating computer viruses or other harmful files</li> <li>Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)</li> <li>Disable/Impair/Disrupt network functionality through the use of computers/devices</li> <li>Using penetration testing equipment (without relevant permission)</li> </ul>						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Corvus Education					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	

On-line gaming (educational)				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce (for school purchases)		X			
File sharing	X				
Use of social media (school accounts)			X		
Use of messaging apps				X	
Use of video broadcasting e.g. You tube (for educational purposes)	X				

### **Staff, Volunteers and Contractors**

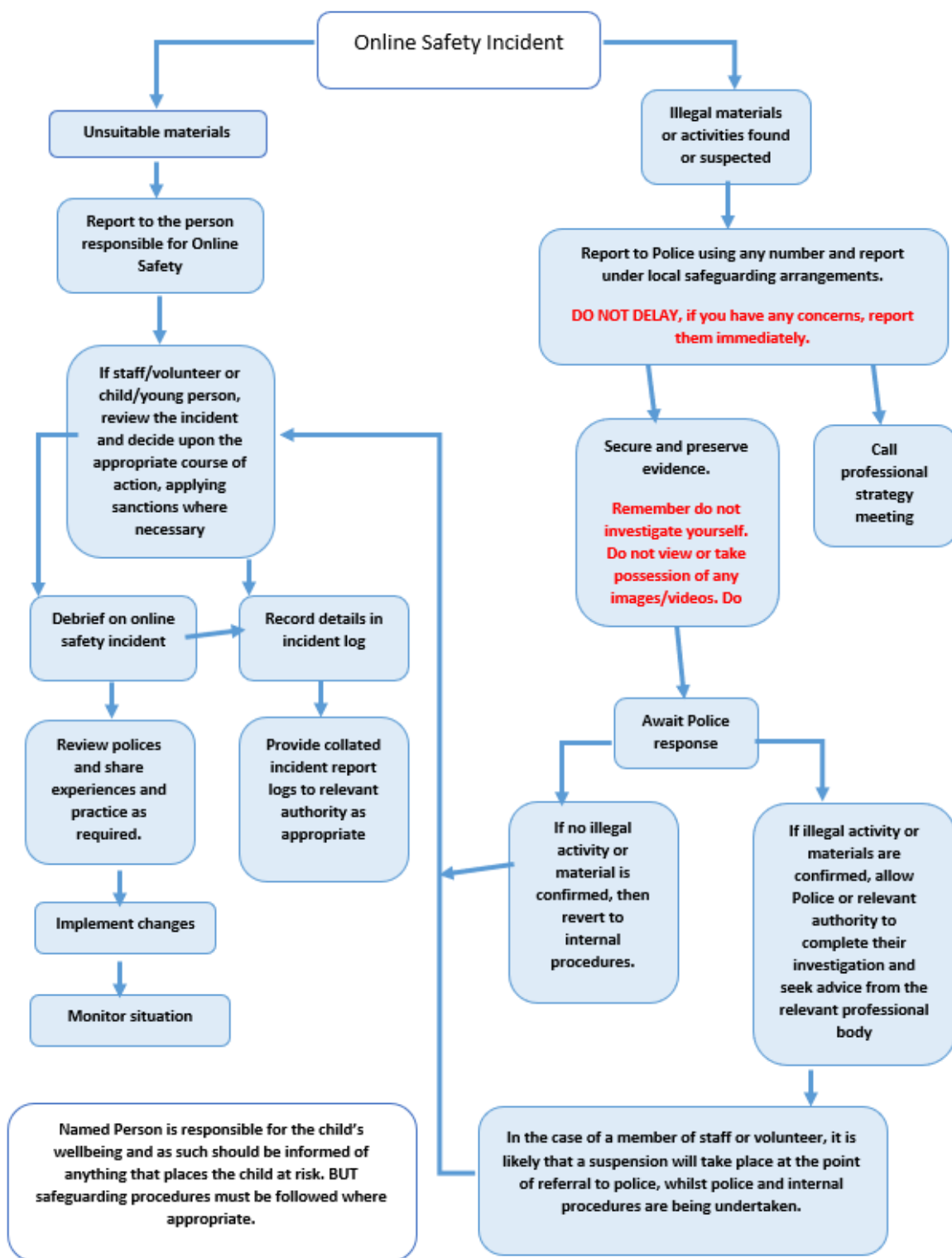
- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications (VLE).
- The use of any school approved social networking will adhere to ICT code of conduct

### **Pupils:**

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our age appropriate Acceptable Use Policy

### *Illegal Incidents*

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



## Other Incidents

It is hoped that all members of the Corvus Education community will be responsible users of digital technologies, who understand and follow Trust's 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 (see User Actions chart 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 that all of the above steps are taken as they will provide an evidence trail for the Corvus Education and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

### **Corvus Education actions & sanctions**

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