Eden Academy Trust
IT and Online Safety Policy
June 2018

Contents

Introduction

In England, academy trusts are subject to an increased level of scrutiny of their online safety practices by Ofsted Inspectors during inspections. From 2015 there are additional duties under the Counter Terrorism and Securities Act 2015 which requires academy trusts to ensure that children are safe from terrorist and extremist material on the internet.

An effective Academy Trust IT & Online Safety Policy must be tailored to the needs of each school and an important part of the process will be the discussion and consultation which takes place during the writing or review of the policy. This will help ensure that the policy is owned and accepted by the whole academy community.

It is suggested that consultation in the production of this policy should involve:

- Members/Trustees/Local Advisory Bodies
- Teaching Staff and Support Staff
- Students/pupils
- Parents
- Community users and any other relevant groups.

Development of this Policy

This IT and Online Safety policy has been developed by a working group made up of the Director of Academy Development, an Academy Associate Head and a representative of the Board of Trustees. The draft policy was reviewed by:

- Headteacher and Head of Schools
- Staff – including Teachers, Therapy staff and Support Staff,
- The Academy Trust's technical support provider
- Local Advisory Bodies
- Parents and Carers

Consultation with the whole Trust community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This IT & Online Safety policy was approved by the Board of Trustees on:	03/05/18
The implementation of this IT & Online Safety policy will be monitored by the:	ICT Review Group Chaired by the Academy Trust Director of Finance and Operations
Monitoring will take place at regular intervals:	
The Board of Trustees will receive a report on the implementation of the IT & Online Safety Policy generated by the ICT Review Group (which will include anonymous details of online safety incidents) at regular intervals:	Twice yearly
The IT & Online Safety Policy will be reviewed annually, 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:	October 2019
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Schools DSL and Academy Trust Designated Safeguarding Lead and in the termly report to the Board of Trustees ICT Contact for LGFL And in exceptional cases to the Local Authority and the Police

The Academy Trust and internet service provider will monitor the impact of the policy using:

- Logs of reported incidents from schools
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity

Scope of the Policy

This policy applies to all members of the Eden Academy Trust Community (including trustees, staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and outside the Trust.

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 academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-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 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The academy 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.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Eden Academy Trust.

1. The Board of Trustees

The Board of Trustees is responsible for the approval of the *IT & Online Safety Policy* and for reviewing the effectiveness of the policy. The Board will review effectiveness by receiving regular information about online safety incidents and monitoring reports from the member of the Board who has taken on the *responsibility of the IT and Online Safet*y as part of the Safeguarding portfolio.

Regular updates and information will be provided by the Director for Schools to the trustee with responsibility for online safety and safeguarding including:

- regular monitoring of online safety incident logs
- access to filtering / change control logs
- reporting serious incidents so that these can be communicated to the Board

2. Headteacher / Director for Schools and Senior Leaders

- The Head 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 member of staff.
- The Head and (at least) another member of the Senior Leadership 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. See the Dealing with Allegations of Abuse against staff guidelines.
- The Head is responsible for ensuring that the Online Safety teacher and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. See Online Safety guidelines for staff, parents and carers.
- The Head 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. Support will be provided by the external ICT support provider.
- The Director of Schools will receive regular reports on matters of online safety from Heads.

3. Network Manager / Technical staff

The Trust's Network Manager, AzteQ is responsible for ensuring:

- that the Trust's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Trust meets required online safety technical requirements and the Eden Academy Trust IT and Online Safety policy

- that users may only access the networks and devices through an appropriate password protection policy
- the filtering policy, is applied and updated on a regular basis appropriate for each school
- 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 network, internet, Learning Platform, remote access, email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Head of School for investigation / action / sanction

4. Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Eden Academy Trust IT and Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or Head of School or designated E Safety Coordinator / Officer for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level *and only carried out using official school systems See Academy Safeguarding Policy and Guidance for Safer Working Practice*
- online safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the IT & Online Safety Policy guidelines as appropriate
- the whole school community have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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
- Whenever the internet is used pupils should be guided to sites suitable for their use and that processes are in place for dealing with any unsuitable material from internet searches.

5. 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
- cyber-bullying

6. Online Safety Group

The Online Safety Group will assist the Trust's E Safety Coordination with:

- The production / review / monitoring of the school E Safety Policy and documents.
- the production / review / monitoring of the school filtering policy (if the school chooses to have one) and requests for filtering changes
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the online safety provision.

7. Students / Pupils

- are responsible for using the Trust's digital technology systems in accordance with the Student / Pupil 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 cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's IT and Online Safety Policy covers their actions out of school, if related to their membership of the school

8. 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. The Trust will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, Learning Platform and information about national and local e safety campaigns or literature. Parents and carers will be encouraged to support the Trust in promoting good e 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 / academy (where this is allowed)

9. Community Users

Community Users who access Trust systems as part of the wider Trust provision will be expected to sign a **Community User AUP** which is under development before being provided with access to Trust systems.

Policy Statements

Education – Students / Pupils

The policy statement relevant to students and pupils are contained in the Eden Academy Trust User Guidelines.

Education – Parents / Carers

Many parents and carers may 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 the children's on-line 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.

Eden Academy Trust 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
- Reference to the relevant web sites and publications (links on Website)

Education & 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:

- **A planned programme of formal online safety training annually and as part of induction will be made available to staff. Schools will keep records of the training delivered**
- **All new staff should receive e safety training as part of their induction programme, ensuring that they fully understand the Eden Academy Trust IT and 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.
- This Online Safety policy and its updates will be presented to and discussed by staff

Training – Members/ Trustees and Local Advisors

Members, Trustees and Local Advisors should take part in e safety training sessions, with particular importance for those with responsibility for Safeguarding or members of the ICT Review Group. This may be offered in a number of ways:

- Attendance at external training courses
- Participation in Eden Academy Trust training or information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The Eden Academy Trust will be responsible for ensuring that the academy 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:

- **Trust technical systems will be managed in ways that ensure that the academy meets recommended technical requirements**
- **There will be 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.**
- **Users (where appropriate) will be provided with a username and secure password by a named member of staff (Key Contact).**
- **Users are responsible for the security of their username and password periodically**
- The "master / administrator" passwords for the Eden Academy Trust ICT system, used by the Network Manager (or other person) must also be available to the Head of School and kept in a secure place
- The Eden Academy Trust external ICT provider 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.
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband provided by The London Grid for Learning by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. **Requests for filtering changes must be made through the Head of School or Head Teacher.**
- **Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- The Trust has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students) **Requests for filtering changes must be made by the Head of School** or Head Techer
- Eden Academy Trust's ICT provider regularly monitors and records 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, as agreed. (ref: Page 23)
- 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 workstations are protected by up to date virus software.
- 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.

- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (to be described) 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**.

Mobile Technologies

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

All users should understand that the primary purpose of the use mobile and personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education programme.

- **The Eden Academy Trust Acceptable Use Agreements for staff, pupils/students and parents/ carers will give consideration to the use of mobile technologies**
- **The Eden Academy Trust allows the use of personal devices for school business (email, Schoolwork) but not for the storage of images.**

Personal devices:

- **Users are allowed to use personal mobile devices in break times and for school business (staff / pupils / students / visitors)**
- **Taking / storage / use of images is not permitted on personal devices**
- **The Trust's policy regarding the use of mobile devices is included in the Staff Acceptable Use Agreement**
- **Personal devices will be keep out of sight of children and not used in classrooms**
- **Access to school Wi-Fi can be available for Personal devices using a Guest access.**
- **The Trust is not Liable for loss/damage or malfunction following access to the network**
- **Technical support will not be available for personal devices**
- **The Trust has the right to take, examine and search user devices in the case of misuse following the recommended legal guidelines**

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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, staff should inform and educate students / pupils 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 permission from parents or carers will be obtained before photographs of students / pupils 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 Trust 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 / pupils* in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school academy policies concerning the sharing, distribution and publication of those images. **Those images should only be taken on Trust equipment, the personal equipment of staff should not be used for such purposes.**
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school / academy into disrepute.
- Students / pupils 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' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Please Note: The Data Protection Act is being replaced by the General Data Protection Regulations which come into force on 25th May 2018. Eden Academy Trust will scrutinise the new regulations to ensure that the latest requirements are incorporated in the IT and Online Safety Policy

Currently, personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Eden Academy Trust must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing"**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data transfer / storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- **the data must be encrypted and password protected**
- **the device must be password protected**
- **the device must offer approved virus and malware checking software**
- **the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete**

Communications

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

When using communication technologies Eden Academy Trust considers the following as good practice:

- **The official Trust email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and students / pupils should therefore use only the school / academy email service to communicate with others when in school, or on school / 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 staff and students / pupils 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) school / academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual academy email addresses for educational use.* (To be amended as appropriate to meet the varying needs of our children in different situations)
- *Students / pupils 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 school / academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the academy and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. Ofsted's online safety inspection framework reviews how an academy protects and educates staff and pupils in their use of technology, including the measures that would be expected to be in place to intervene and support should a particular issue arise. Academies are increasingly using social media as a powerful learning tool and means of communication. It is important that this is carried out in a safe and responsible way.

All schools, Trusts and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Trusts could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The Trust 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

Eden Academy Trust 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 Eden Academy Trust
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official Eden Academy Trust 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 the Eden Academy Trust 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 Eden Academy Trust or impacts on the Trust, it must be made clear that the member of staff 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 Eden Academy Trust 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 Trust should effectively respond to social media comments made by others according to a defined policy or process

The Trust's use of social media for professional purposes will be checked regularly by the senior risk officer and or E Safety Group to ensure compliance with the school policies.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from academy and all other technical systems. Other activities e.g. cyber-bullying is inappropriate behaviour and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in the academy context, either because of the age of the users or the nature of those activities.

Eden Academy Trust believes that the activities referred to in the following section would be inappropriate in the academy context and that users, as defined below, should not engage in these activities either in or outside the Trust when using Trust equipment or systems. The Eden Academy Trust 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, material, remarks, proposals or comments that contain or relate to:	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
	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

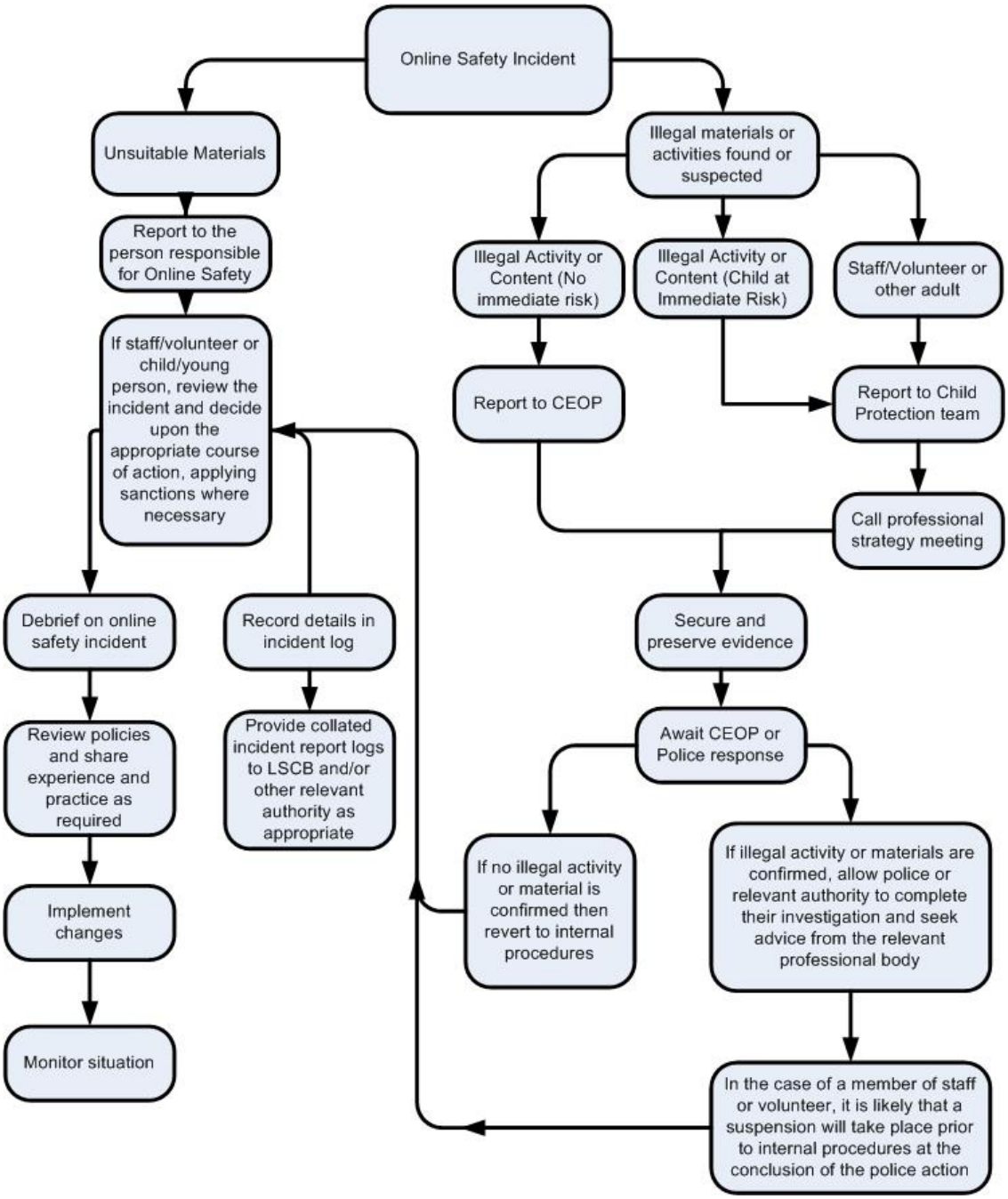
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business						x
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright						x
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files						x
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing				X		
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. You tube				X		

Responding to incidents of misuse

This guidance is intended for use when staff 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 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 (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the Eden Academy Trust 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 member of staff or local Advisor 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. Involve the technical service provider where appropriate.
- 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 the Academy Group
    - 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
    - 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 academy 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.

Eden Academy Trust Actions & Sanctions

It is more likely that the Trust 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.

As well as the Actions and sanctions for student incidents identified below, each school will have agreed sanctions depending on the behaviour identified.

As well as the actions and sanctions for Staff incidents identified below, schools will need to follow the Academy Disciplinary Policy

The Trust or schools within the Trust will take advice for the Local Authority Designated Officer for Safeguarding

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg 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		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 school / academy network by			x			x			

sharing username and passwords									
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			
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			
Continued infringements of the above, following previous warnings or sanctions			x	x		x			
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school			x			x			
Using proxy sites or other means to subvert the academy's filtering system			x		x	x			
Accidentally accessing offensive or pornographic material and failing to report the incident			x		x	x			
Deliberately accessing or trying to access offensive or pornographic material			x	x		x			
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x	x		x			

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	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				
Inappropriate personal use of the internet / social media / personal email		x						
Unauthorised downloading or uploading of files		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						
Careless use of personal data e.g. holding or transferring data in an insecure manner		x						
Deliberate actions to breach data protection or network security rules		x		x				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x	x					
Actions which could compromise the staff member's professional standing		x						
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		x						

Using proxy sites or other means to subvert the academy's filtering system		x			x			
Accidentally accessing offensive or pornographic material and failing to report the incident		x			x			
Deliberately accessing or trying to access offensive or pornographic material		x	x		x			
Breaching copyright or licensing regulations		x	x					
Continued infringements of the above, following previous warnings or sanctions		x	x					