The Bishop Konstant Catholic Academy Trust

Learning Communities, Inspired by Faith

Trust E-Safety Policy

The Bishop Konstant Catholic Academy Trust,
St Wilfrid's Catholic High School & Sixth Form College,
Cutsyke Road, Featherstone WF7 6BD
Telephone: 01924 802285
Email: admin@bkcat.co.uk **Website:** www.bkcat.co.uk

POLICY DOCUMENT	Trust E-Safety Policy
Legislation/Category: Academy Schools	**Required**
Lead Member of Staff:	Trust IT Service Team Leader
Approved by:	BKCAT Board
Date Approved:	March 2023
Revision Date:	March 2024
Review Frequency:	Annual

Mission Statement

All policies are written in line with our Trust Mission statement:

With Jesus Christ at the centre of the life of the Trust, we seek to provide learning communities offering the highest possible standards of education. We are committed to working in partnership and trust for the common good. We strive to encourage and empower children and young people to recognise and realise their God-given potential and to discern their vocation in life. As learning communities inspired by faith, we celebrate achievement, offering each other challenge and support, as together we follow Christ in self-giving love and service.

Change Control

Version	*Date*	*Author*	*Changes*
1.2	***9/8/2022***	***CTU***	***Update to reference Trust Personal Electronic Devices*** ***Change of flow chart (pg 17)to inform HR at an earlier stage for staff issues*** ***Pg 12 now refers to the Trust GDPR Policy, instead of the Data Protection Act.***
1.1	*31/12/2021*	CTU	*Page 14, Updates to links.* *Appendix 1, added HR email address for Staff incidents.*
1.0			Original Approved Document

Contents

Introduction

The internet and other digital and information technologies are vehicles for a wide range of opportunities for both staff and students/pupils in the Trust. Electronic communication has become a regular teaching tool and can promote stimulating and effective learning. The staff and students/pupils of the Trust should have an entitlement to safe internet access at all times.

The requirement to ensure that staff and students/pupils are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in academies are bound. The Trust E-Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in the educational setting from the Headteacher and governors to the senior leaders, classroom teachers, support staff, parents, members of the community and the students/pupils themselves.

Although the use of these exciting and innovative tools has created opportunities for advancement these new technologies can put young people at risk within and outside the academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

It is very difficult to remove all these risks completely. It is therefore essential, through training and educational provision to make staff and students/pupils aware of the risks to which they may be exposed, so that they are informed and skilled to manage any potential risk, if it were to occur. The Trust wishes to ensure that the educational culture within the organisation encourages responsible and positive usage of the internet.

Who is the Policy for?

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

The Education and Inspections Act 2006 empowers Headteachers, 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 E-Safety incidents covered by this policy, which may take place out of the academy, but is linked to membership of the academy.

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the academies:

Governors:

Governors are responsible for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including E-Safety) of members of the school community.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff. (see flow chart on dealing with E-Safety incidents – included in a later section – "Responding to incidents of misuse" and relevant HR / disciplinary procedures).

The Academy Leader with responsibility for Child Protection and Safeguarding:

The leader with responsibility for child protection and safeguarding should be trained in E-Safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data;
- Access to illegal / inappropriate materials;
- Inappropriate on-line contact with adults / strangers;
- Potential or actual incidents of grooming;
- Cyber-bullying;

and they:

- Take day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the academy E-Safety policies / documents;
- Ensure that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident having taken place;
- Provide training and advice for staff;
- Liaise with the Local Authority;
- Liaise with ICT technical staff;
- Receive reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments;
- Report regularly to the Headteacher;

The Trust IT Manager and Trust IT Support Staff:

The Trust IT Manager and Trust IT support staff are responsible for ensuring:

- That the academy's ICT infrastructure is secure and is not open to misuse or malicious attack;
- That the academy meets the E-Safety technical requirements outlined in the Acceptable Usage Policy;
- That users may only access the academy's networks through a properly enforced password protection policy;
- Appropriate and effective filtering is agreed on and in place;
- That monitoring software / systems are implemented and updated as agreed in academy policies.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of E-Safety matters and of the current academy E-Safety policy and practices;
- They have read, understood and signed the Staff Acceptable Use Policy (AUP);
- They report any suspected misuse or problem to the relevant senior leader for investigation / action / sanction;
- Digital communications with students/pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official academy systems;
- E-Safety issues are embedded in all aspects of the curriculum and other academy activities;
- Students/pupils understand and follow the academy E-Safety and acceptable use policy;
- Students/pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extra-curricular and extended academy activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current academy policies with regard to these devices;
- In lessons where internet use is pre-planned students/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;

Students/Pupils:

Students/pupils are responsible for ensuring that they:

- Use the academy ICT systems in accordance with the Student Acceptable Use Policy, which they have to sign before being given access to academy systems;
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Know and understand academy policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand academy policies on the taking / use of images and on cyber-bullying;
- Understand the importance of adopting good E-Safety practice when using digital technologies out of the academy and realise that the academy's E-Safety Policy covers their actions out of the academy, if related to their membership of the academy;
- Know who to speak to in order to raise the alarm over any E-Safety issue.

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children are. The academy will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local E-Safety campaigns and literature. Parents and carers will be responsible for:

- Endorsing the Student Acceptable Use Policy;
- Accessing the Academy website or other services the Trust/Academy provide in accordance with the relevant Acceptable Use Policy.

Community Users

Community Users who access Academy/Trust ICT systems / website / VLE as part of the Extended School provision are expected to sign a similar AUP as above before being provided with access to academy systems.

Policy Statements

Education – Students/Pupils

The education of students/pupils at the Trust in E-Safety is an essential part of the Academy E-Safety provision. Students/pupils need the help and support of the academy to recognise and avoid E-Safety risks and build their resilience.

E-Safety education is provided in the following ways:

- E-Safety lessons are provided as part of ICT and Computing lessons and the PSHE programme and other appropriate lessons. This should cover both the use of ICT and new technologies in the academy and outside of the academy;
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities;
- Students/pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students/pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. *N.B. additional duties for academies under the Counter Terrorism and Securities Act 2015 which requires academies to ensure that children are safe from terrorist and extremist material on the internet.*
- Students/pupils are encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside the academy;
- Students/pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Guidelines and information specifically for students/pupils are accessible on the academy website;
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices;
- Where students/pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

The most important lesson is that students/pupils should know whom to speak to if they see or hear about any potential E-Safety issue that they feel uneasy about or are unhappy with.

Education – Parents and Carers

Parents and carers have an essential role in the education of their children in the use of new technologies and in the monitoring / regulation of the children's on-line experiences. Parents may underestimate how often students/pupils and young people come across potentially harmful and inappropriate material on the internet and may be unsure about

what they would do about it. The academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters etc. and there is specific guidance and information available to them from the academy;
- E-Safety training which may be offered and provided by the academy on-site or they may be signposted to external providers.

Education & Training – Staff

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

- A planned programme of E-Safety training is made available to staff via the CPD provision
- IT support staff will receive regular updates through bulletins and training sessions and review guidance documents.

Training – Governors

Governors should take part in E-Safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in ICT / E-Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by relevant organisations
- Participation in training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

- The Trust IT Team and academy will together 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 E-Safety responsibilities;
- Academy ICT systems will be managed in ways that ensure that they meet the E-Safety technical requirements outlined in the Acceptable Usage Policy;
- Servers, wireless systems and cabling must be securely located and physical access restricted where possible;
- All users will have clearly defined access rights to Academy ICT systems;
- All users will be provided with a username and password by IT who will keep an up to date record of users and their usernames as supplied by the Academies. Users will be encouraged to change their password when required;
- Users will be made responsible for the security of their own username and password; they must not allow other users to access the systems using their log on

details and must immediately report any suspicion or evidence that there has been a breach of security;

- The academy will maintain an effective filtering service;
- In the event of the Trust IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher;
- Where possible remote management tools are used by staff to control workstations and view user's activity;
- An appropriate system is in place for users to report any actual/potential E-Safety incident to a relevant person;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, hand held devices etc. from accidental or malicious attempts, which might threaten the security of the academy systems and data;
- The academy infrastructure and individual workstations are protected by up to date virus software;
- Personal data should not be sent over the internet or taken off the academy site unless safely encrypted, or otherwise secured.

Curriculum

E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages in the use of ICT across the curriculum:

- In lessons where internet use is pre-planned, it is best practice that students/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;
- Where students/pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the students/pupils visit;
- It is accepted that from time to time, for good educational reasons, students/pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Manager (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Trust General Data Protection Regulation (GDPR) Policy

Personal data will be recorded, processed, transferred, and made available according to the Trust General Data Protection Regulation (GDPR) Policy. A brief overview is beloe.

Policy

- 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;

Staff must ensure that they:

- At all times, take care to ensure the safekeeping 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, USB stick or any other removable media:

- The data must be encrypted and password protected;
- The device must be password protected (note: many memory sticks / cards and other mobile devices cannot 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 academy policy (below) once it has been transferred or its use is complete.

Communication Technologies

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

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in the academy, or on academy systems (e.g. by remote access);
- Users need to be aware that email communications may be monitored;
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening, or bullying in nature and must not respond to any such email;
- Any digital communication between staff and students/pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications;
- Students/pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- Personal information should not be posted on the academy website and only official email addresses should be used for identification and communication with members of staff.

Personal Electronic Devices

Please see the Trust Personal Elcetronic Devices Policy regarding personal devices

Social Media Policy

Please See the Trust Social Media Policy for information about Social Media.

Acceptable Use Policy

Please see the Trust Acceptable Use Policy and Procedure.

Remote Learning Policy

Please see the Trust Remote Learning Policy.

Dealing with unsuitable/inappropriate activities

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

The Trust or Academy believes that the activities referred to in the following section would be inappropriate in a Trust or Academy context and that users, as defined below, should not engage in these activities in/or outside the Trust or Academy when using Trust or Academy equipment or systems. The Trust or Academy 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	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					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

that contain or relate to:	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: Gaining unauthorised access to school networks, data and files, through the use of computers/devices Creating or propagating computer viruses or other harmful files Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) Disable/Impair/Disrupt network functionality through the use of computers/devices Using penetration testing equipment (without relevant permission) N.B. Schools/academies will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
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			

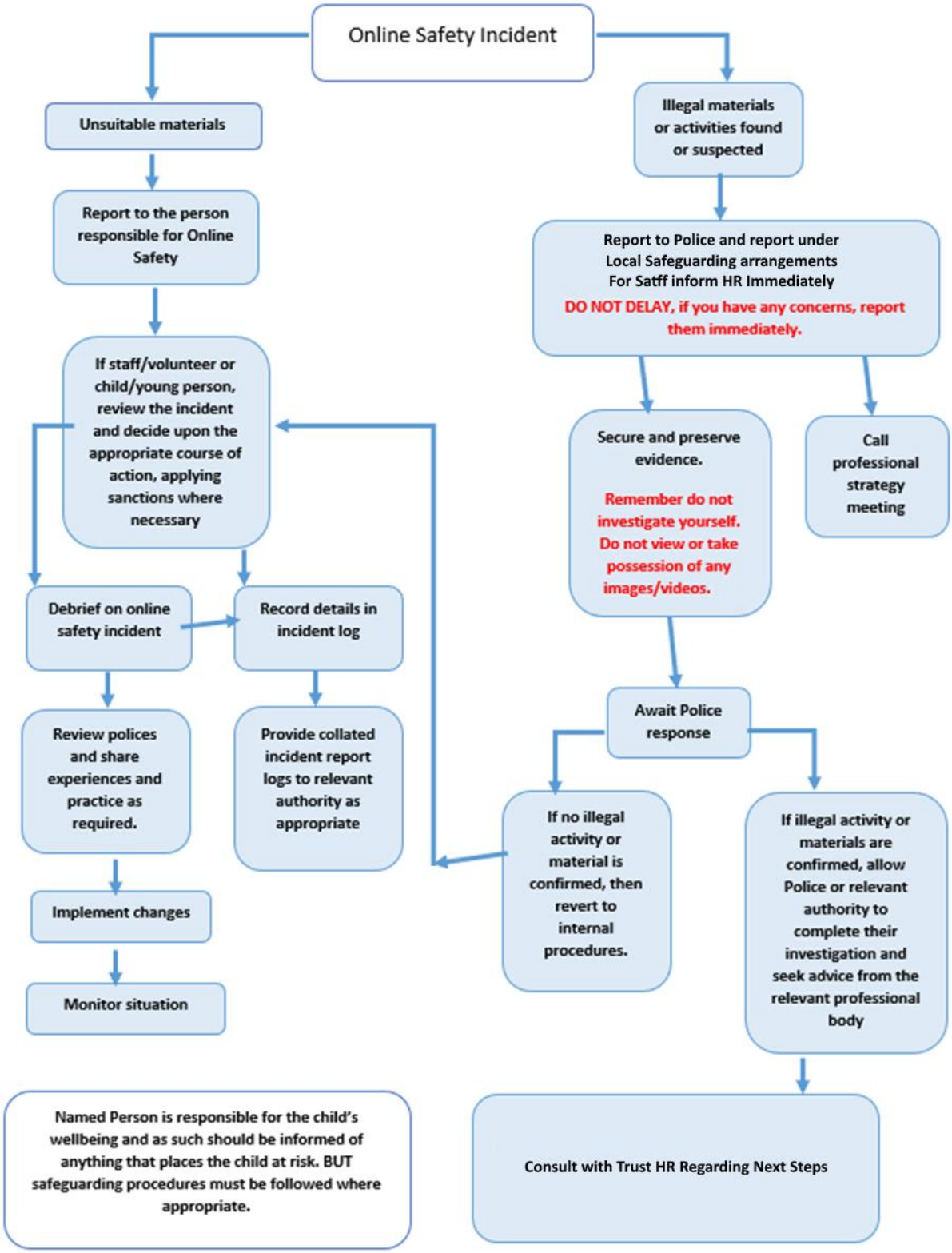
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

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.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police and report under Local Safeguarding arrangements
For Satff inform HR Immediately
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos.
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
Consult with Trust HR Regarding Next Steps

Other Incidents

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

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

- Have more than one senior 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;
- Ensure that the relevant staff 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 *Trust or Academy* and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

Monitoring and Review of this Policy

The Trust shall be responsible for reviewing this policy from time to time to ensure that it meets legal requirements and reflects best practice.

Appendix 1

Academy Actions & Sanctions

It is more likely that the 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.

The academy should use the table below as a template to include its own behaviour sanctions, to ensure appropriate sanctions are in place:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Head of … <please Insert>	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	Warning	Further sanction e.g.
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons									
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device									
Unauthorised/inappropriate use of social media/ messaging apps/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access Trust or Academy network by sharing username and passwords									

Attempting to access or accessing the Trust or Academy network, using another student's/pupil's account									
Attempting to access or accessing the Trust or Academy network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the Trust or Academy into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's/academy's filtering system									
Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

Staff Incidents

Staff incidents should also be refereed to Trust HR on hradvice@bkcat.co.uk.