TDAP044B

E-SAFETY POLICY

Requisite: Dorcan Requirement			Responsible Committee: Full Governing Body		
Vers.	Approval Date	Committee	Head	Chair	Next Review Date
A	19/06/2017	Finance and Premises			01/02/2019
B	18/06/2018	Finance and Premises			November 2022

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within an academy and in their lives outside.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people 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 ineducation settings are bound. An academy e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in an academy and at home has been shown to raise educational standards and promote student achievement. However, the use of 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.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other academy policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

SCOPE OF THE POLICY

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

The Education and Inspections Act 2006 empowered Headteachers, to such extent as is reasonable, to regulate the behaviour of Students 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 academy, but is linked to membership of the academy.

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 e-safety behaviour that take place out of academy.

ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the academy:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the Governing Body

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the academy community, although the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Headteacher and Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in academy who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.
- The Headteacher and the Child Protection Officer/Designated Safeguarding Lead 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.

E-Safety Coordinators (Pastoral Leaders):

- 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 taking place.
- provide training and advice for staff
- liaise with the Local Authority
- liaise with academy ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meet regularly with e-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attend relevant meeting / committee of Governors
- report regularly to Senior Leadership Team

Network Manager:

The Network Manager is responsible for ensuring:

- that the academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the academy's meets the e-safety technical requirements outlined in the Academy's Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the academy's networks through a properly enforced password protection procedure, in which passwords are regularly changed
- the academy's filtering procedure (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in academy policies

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 procedure and practices
- they have read, understood and signed the academy Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator for investigation / action / sanction
- digital communications with students (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 understand and follow the academy e-safety and acceptable use policy
- students 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 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 / Child Protection Officer

- 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

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

E-Safety Committee (Part of Safeguarding/Pastoral Leadership Meetings)

Members of the E-safety committee (or other relevant group) will assist the E-Safety Coordinator / Officer (or other relevant person, as above) with:

- the production / review / monitoring of the academy e-safety policy / documents.
- the production / review / monitoring of the academy filtering procedure

Students:

- are responsible for using the academy ICT systems in accordance with the Acceptable Use Policy, that they will be expected 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
- 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 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.
- should understand the importance of adopting good e-safety practice when using digital technologies out of academy and realise that the academy's E-Safety Policy covers their actions out of academy, if related to their membership of the academy

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 information technology than their children. 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 / literature. Parents and carers will be responsible for:

- endorsing (by signature) the Acceptable Use Policy
- accessing the academy website and VLE in accordance with the relevant academy Acceptable Use Policy.

Community Users

Community Users who access academy ICT systems / website / VLE as part of the Extended Academy provision will be expected to sign a Community User AUP before being provided with access to academy systems.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

POLICY STATEMENTS

Education – students

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

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in academy and outside academy
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be 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 should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside academy
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents / carers

Many parents and carers have only a limited understanding of e-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 on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The academy will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site, VLE
- Parents evenings

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Education - Extended Schools

The academy will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

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 formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.** It is expected that some staff will identify e-safety as a training need within the performance management process.
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the academy e-safety policy and Acceptable Use Policies**
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA /LA and others.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training as required to individuals as required

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 the Local Authority / National Governors Association or other relevant organisation.
- Participation in academy training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The academy 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 e-safety responsibilities:

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

- Academy ICT systems will be managed in ways that ensure that the academy meets the e-safety technical requirements outlined in the Academy's Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- There will be regular reviews and audits of the safety and security of academy ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- **All users will have clearly defined access rights to Academy ICT systems.** Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety Committee (or other group).
- **All users will be provided with a username and password** by the Network Manager who will keep an up to date record of users and their usernames.
- **The "master / administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. academy safe)**
- Users will be made responsible for the security of their username and password. Users 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 maintains and supports the managed filtering service.
- The academy has provided enhanced user-level filtering through the use of the Impero filtering programme.
- In the event of the Network 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 (or other nominated senior leader).
- Any filtering issues should be reported immediately to the ICT Support Team.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and ICT Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- Academy ICT technical staff regularly monitor and record the activity of users on the academy ICT systems and users are made aware of this in the Acceptable Use Policy.
- Remote management tools, such as Impero, are used by selected staff to control workstations and view users activity
- The Network Manager should be contacted to report any actual / potential e-safety incident.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data.
- The ICT Support Department have accounts and passwords with varying levels of access for 'guest' access to the system. These can be obtained from the ICT Support Department and used by persons who are not part of the Dorcan 'community'. Executable files should not be downloaded by users and are prevented from doing so by the academy's filters. Software Restriction Policies are also in place to prevent executable files from being run on

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

unauthorised areas of the computers and networks. Any attempt to circumvent these measures would be considered a breach of the AUP.

- Academy Laptops and other personal devices should not be used by members of their families to ensure the security of Academy data.
- Users are not allowed to install programs on Academy workstations and/or portable devices. All software is to be installed by and at the discretion of the ICT Support Department and only when appropriate software licenses can be proved to be valid and/or purchased. Also, any software that needs to be installed needs to be tested by ICT Support to ensure it is compatible with the Academy network.
- Removable Media (eg memory sticks, CDs, DVDs) are permitted within the Academy but users should take every care to ensure that they are free from harmful software (eg. Viruses, Malware, etc). Software Policies in place ensure that no executable files can be run from these devices and Anti-Virus software will scan as required. However, these devices should not be used to store and transfer any personal identifiable information or sensitive data unless it is encrypted.
- The academy infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot 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 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 are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit; in particular Google Images which, due to its nature, is hard to accurately filter.
- It is accepted that from time to time, for good educational reasons, students 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 Network 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.
- Students should be 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: (select / delete as appropriate)

- **When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- Staff are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the academy website (this is covered as part of the agreement signed by parents or carers at the start of the year).
- Student's work can only be published with the permission of the student and parents or carers.
- Users should be aware of the additional storage demands of digital and video files. As such, files that are no longer required or wanted should be deleted.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and 2018, and the General Data Protection Regulation 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.

Following a number of "high profile" losses of personal data by public organisations, academies are likely to be subject to greater scrutiny in their care and use of personal data.

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, and following the requirements of the Academy GDPR policy and related IT policies**
- **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.**
- **Have obtained consent for the use of the data**

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 (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 procedure 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 academy currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Communication technologies	Staff and other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the academy	✓				✓			
Use of mobile phones in lessons				✓			✓	
Use of mobile phones in social time		✓				✓		
Taking photos on mobile phones or other camera devices		✓	✓					✓
Use of hand held devices e.g. PDAs, PSPs		✓				✓		
Use of personal email addresses in the academy, or on the academy network		✓						✓
Use of the academy email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites			✓					✓
Use of blogs				✓			✓	

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

- **The official academy email service may be regarded as safe and secure and is monitored.** Staff and students should therefore use only the academy email service to communicate with others when in the academy, or on the 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.**

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

- **Any digital communication between staff and students or parents / carers (email, 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 will be provided with individual academy email addresses for educational use.
- Students 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 to identify members of staff.

Unsuitable / inappropriate activities

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

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

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

User Actions

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:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					✓
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					✓
Adult material that potentially breaches the Obscene Publications Act in the UK					✓
Criminally racist material in the UK					✓
Pornography				✓	
Promotion of any kind of discrimination				✓	
Promotion of racial or religious hatred				✓	
Threatening behaviour, including promotion of physical violence or mental harm				✓	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute				✓	
Using academy systems to run a private business				✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy				✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					✓
Creating or propagating computer viruses or other harmful files					✓
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				✓	
	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
On-line gaming (non-educational)				✓	
On-line gambling				✓	
Use of social networking sites				✓	
File sharing			✓		
On-line shopping / commerce		✓	✓		
On-line gaming (educational)		✓			
Use of video broadcasting e.g. YouTube		✓	✓		

Responding to incidents of misuse

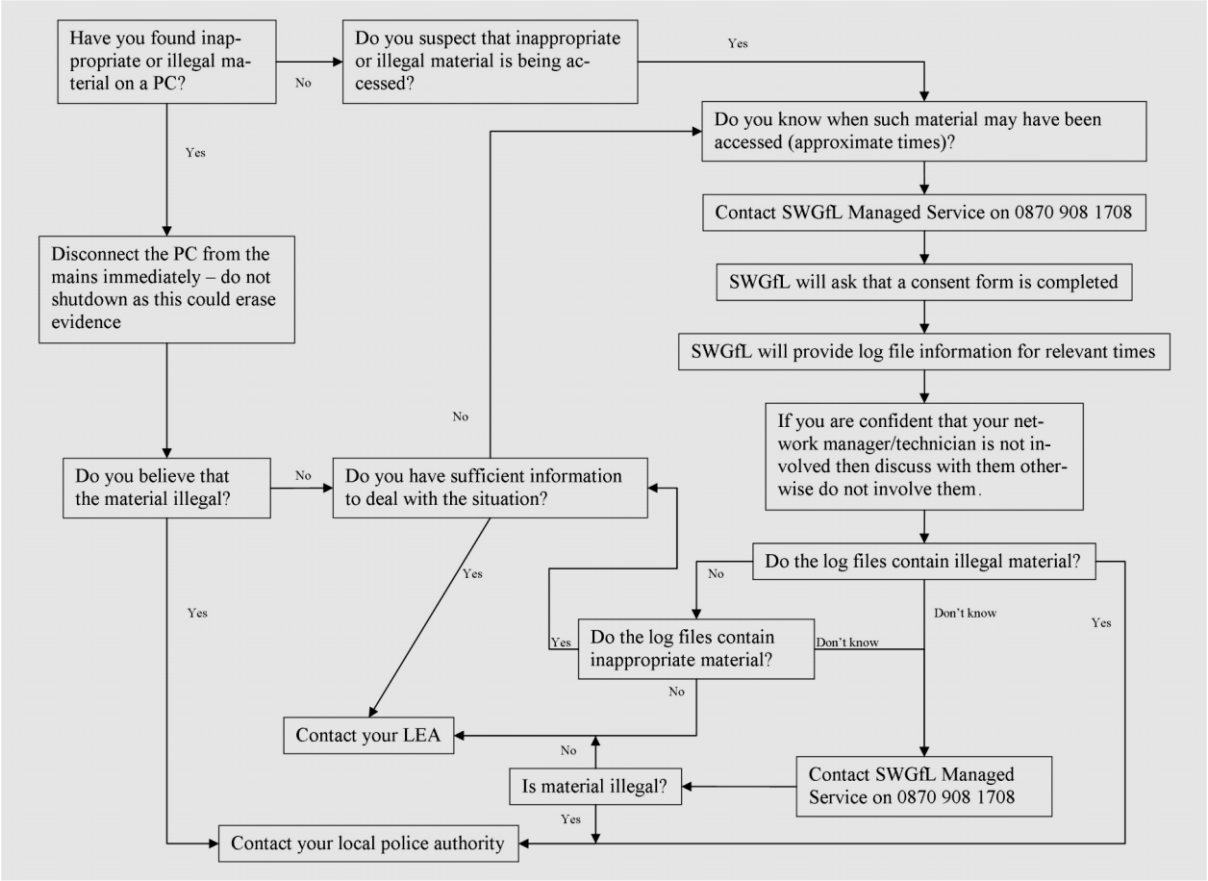
It is hoped that all members of the academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity, i.e.

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

then the SWGfL flow chart (below) should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" should be followed. This can be found on the SWGfL Safe website within the "Safety and Security booklet". This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer.

It is more likely that the academy will need to deal with incidents that involve inappropriateness 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 academy 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 as outlined in Appendices 1 and 2 (for students and staff respectively).

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

MONITORING & REVIEW

This e-safety policy has been developed by relevant academy staff and has been approved by the Finance and Premises Committee and ratified by the Full Governing Body. This policy will be monitored and reviewed every three years, or sooner if required by legislation.

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

APPENDIX 1 **Actions / sanctions for students** Incidents:	Refer to tutor	Refer to Head of House	Refer to Headteacher	Refer to Police	Refer to Network Manager for action re filtering / security etc.	Inform Parents / Carers	Removal of network / internet access rights	Warning	Further sanction (e.g. detention / exclusion)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓	✓		✓			✓
Unauthorised use of non-educational sites during lessons					✓				
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓			✓			
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓	✓		
Unauthorised downloading or uploading of files	✓				✓				✓
Allowing others to access academy network by sharing username and passwords		✓			✓				✓
Attempting to access or accessing the academy network, using another student's / pupil's account		✓			✓	✓			✓
Attempting to access or accessing the academy network, using the account of a member of staff		✓	✓		✓	✓			✓
Corrupting or destroying the data of other users		✓	✓		✓	✓			✓
Sending an email, text or instant 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 academy into disrepute or breach the integrity of the ethos of the academy	✓	✓			✓	✓			
Using proxy sites or other means to subvert the academy's filtering system		✓			✓		✓		✓
Accidentally accessing offensive or pornographic material and failing to report the					✓				

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

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	✓	✓			✓	✓	✓		✓

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

APPENDIX 2 **Actions / sanctions for staff** Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority	Refer to Police	Refer to Network Manager for action re filtering / security 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).		✓	✓	✓			✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✓				✓			
Unauthorised downloading or uploading of files	✓				✓			
Allowing others to access the academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	✓				✓	✓		✓
Careless use of personal data e.g. holding or transferring data in an insecure manner	✓				✓	✓		
Deliberate actions to breach data protection or network security rules		✓		✓	✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓	✓	✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓			✓
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students		✓	✓	✓			✓	✓
Actions which could compromise the staff member's professional standing		✓	✓	✓			✓	✓
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		✓	✓		✓		✓	✓
Using proxy sites or other means to subvert the 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		✓	✓				✓	✓

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

Breaching copyright or licensing regulations	✓	✓			✓	✓		
Continued infringements of the above, following previous warnings or sanctions		✓	✓			✓	✓	✓

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)

The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies

- Complaints
- Safeguarding Children and Young people
- Behaviour
- Anti-Bullying
- Lettings and Use of Premises
- Special Educational Needs
- Academy trips
- Curriculum
- Children in Care
- Health and Safety
- Sex and Relationships Education
- Security
- Equality Diversity and Community Cohesion
- Students with Additional Needs
- Internet Access and Use
- Use of ICT and Website
- Cloud based
- Password
- GDPR
- Young Carers
- Privacy, Confidentiality, Information Sharing and Data
- Whistle blowing

The above list is not exhaustive but when undertaking development or planning of any kind the academy will consider safeguarding matters.

- **Revision Notes**

New format and amendments

Rev A:	Original

*The Governing Body's legal responsibility for safeguarding the welfare of children goes beyond basic child protection procedures. The duty is now to ensure that safeguarding permeates all activity and functions. This policy therefore complements and supports a range of other policies (Appendix 1)