Online Safety Policy

Contents

Version History

Date	Author	Version	Comment
Oct 2019	Brett Webster	1.0	Approved by Trustees Oct 2019
Aug 2021	Brett Webster	2.0	

1. Policy Development and Review

The Online Safety Policy was developed by the Trust in March 2018. It has been adapted with reference to policy templates from South West Grid for Learning and adapted to meet our needs.

Upon review, the policies below will be consulted to ensure clarity.

- Safeguarding / child protection.
- Anti-bullying
- Behaviour
- Information Security
- Information Governance
- Employee code of conduct / employee's handbook
- Data protection
- Preventing Radicalisation
- Social Media

2. Scope of the Policy

This policy applies to all members of the academy community (including employees, pupils, volunteers, parents / 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 Principals to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the academy site and empowers members of employees 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. 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 academy.

3. Roles and Responsibilities

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

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day to day responsibility for online safety will be delegated to the academy IT Leads.
- The Principal and (at least) another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of employees.
- The Principal and Senior Leaders are responsible for ensuring that the academy IT Leads and other relevant employees receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the academy IT Leads.

Academy IT Lead:

- Leads the Online Safety Group.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the academy online safety policies / documents.
- Ensures that all employees are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for employees.
- Liaises with the Trust and other relevant bodies.
- Liaises with academy IT support employees.
- Receives reports of online safety incidents.
- Meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- Attends relevant meeting / Academy Improvement Committee.
- Reports regularly to Senior Leadership Team

ICT Technical Support

The ICT Technical Support employees are responsible for ensuring:

- That the academy's technical infrastructure blueprint from the Trust is supported, regularly checked, updated, and therefore secure and is not open to misuse or malicious attack.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed in accordance with the Trust Information Governance policy.
- That internet filtering is differentiated according to the age of the person and the needs of the academy.
- 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 academy network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal for investigation / action / sanction.

Teaching and Support Employees

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current academy Online Safety Policy and practices.
- They have read, understood and signed the Employees Acceptable Use Policy (AUP).
- They report any suspected misuse or problem to the Principal for investigation / action / sanction
- All digital communications with pupils / parents / carers should be on a professional level and only carried out using official academy systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Pupils understand and follow the Online Safety Policy and acceptable use policies.
- Pupils 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 academy activities (where allowed) and implement current policies with regard to these devices

- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead

The DSL should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from incidents such as:

- Sharing of personal data.
- Access to illegal / inappropriate materials.
- Inappropriate online contact with adults / strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Refer to the Trust Safeguarding and Child Protection Policy for further information.

4. Education

Pupils

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

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

- A planned online safety curriculum will be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key online safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities.
- Pupils will be taught in all appropriate lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils will 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.
- Pupils will be helped to understand the need for the Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside the academy.
- Employees will act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that 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 pupils are allowed to freely search the internet, employees should be vigilant in monitoring the content of the websites.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet

searches being blocked. In such a situation, employees can request that the Technical employees (or other relevant designated 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.

Parents / Carers

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

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

- Letters, newsletters, web site, social media
- High profile events / campaigns e.g. Safer Internet Day

Employees / Volunteers

It is essential that all employees 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 will be made available to employees through Flick. This will be regularly updated and reinforced. An audit of the online safety training needs of all employees will be carried out annually.
- All new employees will receive online safety training as part of their induction programme, ensuring that they fully understand the academy Online Safety Policy and Acceptable Use Agreements.
- This Online Safety Policy and its updates will be presented to and discussed by employees team meetings / INSET days.

Academy Improvement Committee

Academy Improvement Committees take part in online safety training / awareness sessions. This will be offered via Flick.

5. Technical

The Trust and the academy will be responsible for ensuring that the academy infrastructure / network is as safe and secure as is reasonably possible.

The technical requirements regarding security and integrity of the academy infrastructure and all devices is contained within the Trust Information Governance policy. The following is for clarity and additional information.

- All users will have clearly defined access rights to academy technical systems and devices suitable to their role within the academy.
- The administrator passwords for the academy ICT systems must also be available to the Principal or other nominated senior leader and kept in a secure place (e.g. academy safe).

Internet Filtering

- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that pupils are safe from terrorist and extremist material when accessing the internet.
- The academy has provided differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – employees / pupils etc.)

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on the academy network and on academy equipment using Futures Cloud monitoring software.

Monitoring will take place as follows:

- All devices, including iPads, PC's and laptops are monitored using Futures Cloud.
- All student alerts are sent to the online safety lead and action taken as necessary.
- All employees alerts are sent to the principal and action taken as necessary.
- The employees who monitor the solution in each academy are in turn monitored by nominated personnel within the Trust.

Passwords

- All employees will have various passwords for access onto different systems, e.g. academy network, CPOMS, remote access etc. All passwords will be regularly changed in accordance with the Information Governance policy.
- All pupils (at KS1 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password in accordance with Trust Information Governance policy.

Anti-Virus

- Sophos anti-virus software is used on all appropriate academy devices. This software is automatically and regularly updated.

USB Devices

- The use of USB devices such as backup drives, pendrives etc. is not permitted on academy systems.

Personal Mobile Devices

The term 'personal mobile devices' references the wide range of technology that is now available and will include devices such as:

- Mobile phones / tablets.
- Smart wearable technology (e.g. smart watches).

Employees

Employees are permitted personally owned mobile devices within the academy, however they must be:

- Kept in lockers or in areas of the school that are secluded.
- Used only within secluded areas and away from areas where pupils are permitted to be.
- In the case of smart watches, employees should have notifications switched off to remove the temptation to check.
- Personal devices are not to be used for taking images/videos of the pupils or other members of employees.
- Not used for direct contact with pupils.

Pupils

Pupils are not permitted to use personally-owned mobile devices within the academy. In extraordinary circumstances a small number of children may be permitted to bring a device to the academy (e.g. a mobile phone) however this should be handed into reception on arrival at the academy and only done on consultation with the Principal.

Due to the potential for images/videos to be taken in the classroom/playground/toilets etc. children will not be permitted to wear smart watches. If any children are found to be wearing a smart watch they will be asked to remove and leave at reception for collection at the end of the academy day.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing employees and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, employees, parents / carers and 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 academy 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, employees should inform and educate 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 pupils are published on the academy website / social media / local press. These permissions will be obtained annually.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use is not covered by the General Data Protection Regulation). 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 pupils in the digital / video images.

- Employees and volunteers 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 employees should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere.

Social Media

Academy Use

Our academy uses the following social media services in order to promote the academy, the pupils and their learning with parents and the wider community

- Twitter – administered by Mrs T. Dixon

The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, employees and the academy 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.

All information will be moderated before posting, taking into account children who cannot be publicized and the principles of our photos/videos policy.

Protecting Professional Identity

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy /

academy or impacts on the academy/ academy, it must be made clear that the member of employees is not communicating on behalf of the academy with an appropriate disclaimer. Such personal communications are within the scope of this policy

- No reference should be made in social media to pupils, parents / carers or academy employees.
- Do not engage in online discussion on personal matters relating to members of the academy community
- Personal opinions should not be attributed to the academy.
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information

Unsuitable / Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy / 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 an 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 an academy / academy context and that users, as defined below, should not engage in these activities in / or outside the academy when using academy equipment or systems. The academy policy restricts usage as follows:

User Actions			Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users	shall not	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 academy or brings the academy into disrepute				X	
Using academy systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the 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. Youtube				X	

Incident Management

Employees

	Person Responsible
Where there is concern that there has been a breach of the online safety policy the person who is made aware of this will report this to the designated lead for online safety/safeguarding.	Member of Employees aware of the incident
The academy IT Leads will conduct an initial fact finding investigation which will ascertain who was involved, what has occurred. If appropriate the user will be restricted from access to the network.	Principal
The academy IT Leads will classify the incident appropriately (high or low severity) and enter details of the incident onto the member of employees's file.	Principal
The Principal will have been informed and should be given the results of the initial fact finding investigation.	Principal
If appropriate discussions will take place between the Trust Online Team and local ICT Technicians to implement any necessary actions e.g. blocking a website	Principal

The Principal will discuss the concerns with the Local Authority Designated Officer (LADO) in order to discuss whether there is a need for a Strategy Meeting. During this discussion consideration will be given as to whether the police need to be involved. The Principal/Principal of Academy/line manager will also discuss with Lauren Pilgrim (Director of HR) if the member of employees needs to be suspended or undertake different duties pending the completion of the enquiries.	Principal
The Principal of Academy/line manager will also discuss the incident with the Online Safety Lead in the Trust as consideration will need to be given to any further actions required.	Principal
The strategy meeting process will be completed.	
The designated lead will complete the agencies incident log and send a copy to the Trust's Safeguarding Lead	Principal

Pupils

	Person Responsible
Where there is concern that there has been a breach of the online safety policy the adult will make a decision whether to deal with it themselves by applying a sanction and logging it in the relevant systems or report it to the Senior Leadership Team.	Member of Employees aware of the incident
The Senior Leadership Team will conduct an initial fact finding investigation who will ascertain who was involved, what sites have been accessed etc.	Senior Leadership Team with support from the Principal and ICT support
The Senior Leadership Team will classify the incident appropriately (high or low severity) and enter details of the incident into the relevant system and make a decision about appropriate sanctions, with support from the Trust's Safeguarding Team if necessary. They will also inform the ICT Technician's to enable them to make changes	Senior Leadership Team with support from Principal and ICT support

to the computer system if reduced access is required.	
If necessary, the Principal will discuss the concerns with the manager of the local authority safeguarding team to establish if there are child protection concerns requiring a Section 47 Child Protection investigation. If this is required the local Safeguarding Team will conduct this investigation as required within the Child Protection Procedures.	Principal/Principal of Academy

** Disciplinary matters (sanctions) will be in accordance with the **Academy Behaviour Policy**.

Acceptable Use

Employees

Note: All device, Internet and email activity is subject to monitoring.

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking – is allowed in academy in accordance with the online safety policy only. Employees using social networking for personal use should never undermine the academy, employees, parents or children. Employees should not become "friends" with parents or pupils on personal social networks.

Use of Email – employees are not permitted to use academy email addresses for personal business. All email should be kept professional. Employees are reminded that academy data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Employees should keep passwords private. There is no occasion when a password needs to be shared with another member of employees or student, or IT support.

Data Protection – USB drives (e.g. pendrives) are not permitted on the academy network.

Personal Use of Academy ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given by the Principal who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other employees or pupils without consent. This is applicable professionally (in academy) or personally (i.e. employees outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Principal.

Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Online Safety Officer.

Online Safety – like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of employees or with pupils.

NAME: ……..

SIGNATURE: ……..

DATE: ……..

Foundation / KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer / tablet.

Signed (child): .....

Signed (parent): .....

Date: .....

KS2

I Promise

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

I will not

- Use other people's work or pictures without permission to do so.
- Damage the ICT equipment, if I accidentally damage something I will tell my teacher.
- Share my password with anybody. If I forget my password I will let my teacher know.
- Use other people's usernames or passwords.
- Share personal information online with anyone.
- Download anything from the Internet unless my teacher has asked me to.

I will

- Let my teacher know if anybody asks me for personal information.
- Let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
- Be respectful to everybody online; I will treat everybody the way that I want to be treated.

I understand

- That some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in academy, or my parents if I am at home.
- If I break the rules there will be consequences of my actions and my parents will be told.

Signed: .....

Date: .....

Parent / Carer Acceptable Use Agreement Template Letter

Digital technologies have become integral to the lives of children and young people, both within academies and outside academies. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The academy will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect them to agree to be responsible users. A copy of the Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the academy expectations of the pupils in their care.

Parents are requested to sign the permission form to show their support of the academy in this important aspect of the academy's work.

Parent / Carer Permission Form

Parent / Carers Name: .....

Student / Pupil Name: .....

As the parent / carer of the above, I give permission for my son / daughter to have access to the internet and to ICT systems at academy.

Either: (KS2)

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of academy.

Or: (KS1)

I understand that the academy has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of academy.

I understand that the academy will take every reasonable precaution, including monitoring and filtering systems, to ensure that the children will be safe when they use the internet and systems. I also understand that the academy cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the systems will be monitored and that the academy will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the academy if I have concerns over my child's online safety.

Signed: .....

Date: .....

6. National Links

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for academys: www.360safe.org.uk

7. Legislation

Academies should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 2018/General Data Protection Regulation

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line employees.
- The academy reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions employees fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the academy context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The academy is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Principal/teachers, to such extent as is reasonable, to regulate the behaviour of pupils / pupils when they are off the academy site and empowers members of employees to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Principal/teachers (and nominated employees) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance - http://www.education.gov.uk/academys/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires academies to seek permission from a parent/carer to use Biometric systems

The Academy Information Regulations 2012

Requires academies to publish certain information on its website:

https://www.gov.uk/guidance/what-maintained-academys-must-publish-online

Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)