Diocese of Norwich Education and Academies Trust

[Academy Name]

e-Safety and ICT Acceptable Use Policy

Policy Type:	**Trust Core Policy**
Approved By:	**DNEAT Trust Board**
Approval Date:	**18/09/2015**
Date Adopted by LGB:	**dd/mm/yyyy**
Review Date:	**September 2017**
Person Responsible:	**DNEAT Operations Manager**

Summary of Changes

The model policy has been revised to reflect these changes to the statutory guidance as outlined below.

Page Ref.	Section	Amendment	Date of Change
13	Communications	New definition of child sexual exploitation that can occur through use of technology Working Together to Safeguard Children March 2015 ©2017 page 93	March 2017

Roles and Accountabilities

Index

Introduction
The Diocese of Norwich Education and Academies Trust is accountable for all policies across its Academies. All policies whether relating to an individual academy or the whole Trust will be written and implemented in line with our ethos and values as articulated in our prospectus. We are committed to the provision of high quality education in the context of the Christian values of service, thankfulness and humility where individuals are valued, aspirations are high, hope is nurtured and talents released.

A Scheme of Delegation for each academy sets out the responsibilities of the Local Governing Body and Principal / Head Teacher. The Principal / Head Teacher of each academy is responsible for the implementation of all policies of the Academy Trust.

All employees of the Academy Trust are subject to the Trust's policies.
(Insert name) has an overview of e-Safety.
Our e-Safety and ICT Acceptable Use Policy is based on national educational trust guidelines. It has been agreed by the Leadership Team and approved by the Local Governing Body.

Schedule for Development/Monitoring/Review

This e-Safety and ICT Acceptable Use policy was approved by the DNEAT Board of Trustees/adopted by the LGB on……(insert date)

The implementation of this e-Safety and ICT Acceptable Use policy will be monitored by the Safeguarding and Health and Safety Lead Officer/ LGB Safeguarding Governors (insert name/s)

Monitoring will take place at regular intervals: (annually)

The Trustees/LGB will receive a report on the implementation of the e-Safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals (annually mid year)

The e-Safety policy will be reviewed annually or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The anticipated review date will be: (insert date)

Should serious e-Safety incidents take place, the following external persons/agencies be informed (DNEAT Safeguarding&Health and Safety Lead Officer/ Police/Archdeacon of Norwich Jan McFarlane/ ICT Network team)

The academy will monitor the impact of the policy using (delete/add as relevant)

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys/questionnaires of
  -Pupils/students

-Parents/carers
-Staff

Scope of the Policy

This policy applies to all members of the academy community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of academy ICT systems, including digital communication technologies, both in and out of the academy
The Education and Inspections Act (2006) empowers Headteachers/Principals to such an extent as is reasonable, to regulate the behaviour of pupils/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 outside of the academy, but is linked to membership of the academy and the Diocese of Norwich Education and Academies Trust (DNEAT). 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 academy 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 e-Safety behaviour that take place out of the academy.

Roles and Responsibilities

The Board of Trustee are responsible for the approval of the e-Safety policy and with the (insert name of Academy LGB) are responsible for reviewing the effectiveness of the policy. This will be carried out by the Trustees/LGB receiving regular information about e-Safety incidents and monitoring reports. A member of the LGB has taken on the role of e-Safety Governor and the role includes:

- regular meetings with the e-Safety Co-ordinator/Officer
- regular monitoring of e-Safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant LGB/Trust Board/Committee/ meeting

Headteacher/Principal and Senior Leaders

- The Headteacher/Principal has a duty of care for ensuring the safety (including e-Safety) of members of the academy community, though the day to day responsibility for e-Safety will be delegated to the e-Safety Co-ordinator/Officer
- The Headteacher and (at least) another member of the Senior Leadership/Senior Management 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
- The Headteacher/Principal/Senior Leaders are responsible for ensuring that the e-Safety Coordinator/Officer and other relevant staff receive suitable training to enable them to carry out their e-Safety roles and to train other colleagues, as relevant.
- The Headteacher/Principal/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the academy who carry out the internal e-

Safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles.

- The Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the e-Safety Coordinator/Officer

E-Safety Coordinator/Officer

- Leads the e-safety committee (this may be combined with Child Protection/Safeguarding Officer role)
- Takes day to day responsibility for e-Safety issues and has a leading role in establishing and review the academy e-Safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident taking place.
- Provides training and advice for staff
- Liaises with the DNEAT Safeguarding Lead/ relevant body
- Liaises with academy technical staff
- Receives reports of e-Safety incidents and creates a log of incidents to inform future e-Safety developments.
- Meets regularly with e-Safety Governor to discuss current issues. Review incident logs and filtering/change control logs
- Attends relevant meeting/committee of LGB
- Reports regularly to Senior Leadership Team

Network Manager/Technical Staff

For academies who have a managed ICT service provided by an outside contractor it is the responsibility of the academy to ensure the managed service provider carries out all e-Safety measures as outlined below and that the managed service provider is fully aware of the academy e-Safety policy and procedures.

The Network Manager/Technical Staff/ICT Coordinator is responsible for ensuring

- That the academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets required e-safety technical requirements and any Trust / other relevant body E-Safety Policy / Guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy (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
- That they keep 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 / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / Principal / Senior Leader; E-Safety Coordinator / Officer (insert others as relevant) 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 policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- They report any suspected misuse or problem to the Headteacher / Principal / Senior Leader ; E-Safety Coordinator / Officer (insert others as relevant) for investigation / action / sanction
- All digital communications with students / pupils / parents / carers 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 activities
- Pupils/students understand and follow the e-Safety and acceptable use policies
- Pupils/students 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/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

Child Protection / Safeguarding Designated Person / Officer

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

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

Some academies may choose to combine the role of e-Safety Officer with Safeguarding role

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding e-safety and the monitoring the e-safety policy including the impact of initiatives. Depending on the size or structure of the academy this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the LGB and then to the Trust Board.

Members of the E-safety Group (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 policy (if the academy chooses to have one) and requests for filtering changes.
- Mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- Monitoring improvement actions identified

Pupils/Students:

- Are responsible for using the academy digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of 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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will 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 encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at academy events (see Use of Digital Images and Videos policy guidelines below)
- access to parents' sections of the website / VLE and on-line student / pupil records
- their children's personal devices in the academy (where this is allowed)

Policy Statements

Education – students / pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils 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 should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways: (statements will need to be adapted, depending on academy / academy structure and the age of the students / pupils)

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils 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 / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside academy
- Staff should 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 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, staff should be vigilant in monitoring the content of the websites the young people visit.
- 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 Technical Staff (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.

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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The academy will therefore seek to provide information and awareness to parents and carers through: (select / delete as appropriate)

- Curriculum activities
- Letters, newsletters, web site, VLE
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education – The Wider Community

The academy will provide opportunities for local community groups / members of the community to gain from the academy's e-safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and e-safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision

Education & Training – Staff / Volunteers

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: (select / delete as appropriate)

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. 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 Agreements. .
- The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- 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 / Officer (or other nominated person) will provide advice / guidance / training 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 subcommittee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the DNEAT/NGA / National Governors Association / or other relevant organisation.
- Participation in academy training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Use of Digital/Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of academy. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the public media,

When using digital images, staff should inform and educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. The academy will also ensure that when images are published that the young people cannot be identified by the use of their names.

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 in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers will be required to sign a relevant permission form to allow the academy to take and use images of their children and for the parents / carers to agree

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:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements (these may be outlined in DNEAT/ other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password by (insert name or title) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every (insert period). (Academies may choose to use group or class log-on and passwords for KS1 and below, but need to be aware of the associated risks)
- The "master / administrator" passwords for the academy ICT system, used by the Network Manager (or other person) must also be available to the Headteacher / Principal or other nominated senior leader and kept in a secure place (e.g. academy safe)
- (Insert name or role) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the academy to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. (the

academy will need to decide on the merits of external / internal provision of the filtering service – see appendix). There is a clear process in place to deal with requests for filtering changes

- The academy has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / pupils / students etc.)
- Academy technical staff regularly monitors and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement. (Academy's may wish to add details of the monitoring programmes that are used).
- An appropriate system is in place (to be described) for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place (academy's may wish to provide more detail) to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the academy systems and data. These are tested regularly. The academy infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (to be described) for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the academy systems.
- An agreed policy is in place (to be described) regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on academy devices that may be used out of the academy.
- An agreed policy is in place (to be described) that allows staff to / forbids staff from downloading executable files and installing programmes on academy devices.
- An agreed policy is in place (to be described) regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on academy devices. Personal data cannot be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

- The academy has a set of clear expectations and responsibilities for all users
- The academy adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Students / Pupils receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported as in the BYOD policy
- Any user leaving the academy will follow the process outlined within the BYOD policy

Data Protection

The academy must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing". (see Appendix 4)
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

Communications

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. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the academy email service to communicate with others when in the academy, or on academy systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with the academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. This includes any communication linked to Prevent Duty and radicalisation and linked to child sexual exploitation that can occur through the use of technology.
- 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 social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual academy email addresses for educational use.
- Students / pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who

defame a third party may render the academy or DNEAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through limiting access to personal information:

- Training to include: 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

Academy and DNEAT staff should ensure that:

- No reference should be made in social media to students / pupils, parents / carers or academy staff
- They 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 or DNEAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The academy's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications policies and E-Safety and ICT Acceptable Use Policy

Unsuitable / inappropriate activities

The academy believes that the activities referred to in the following section would be inappropriate in an 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:

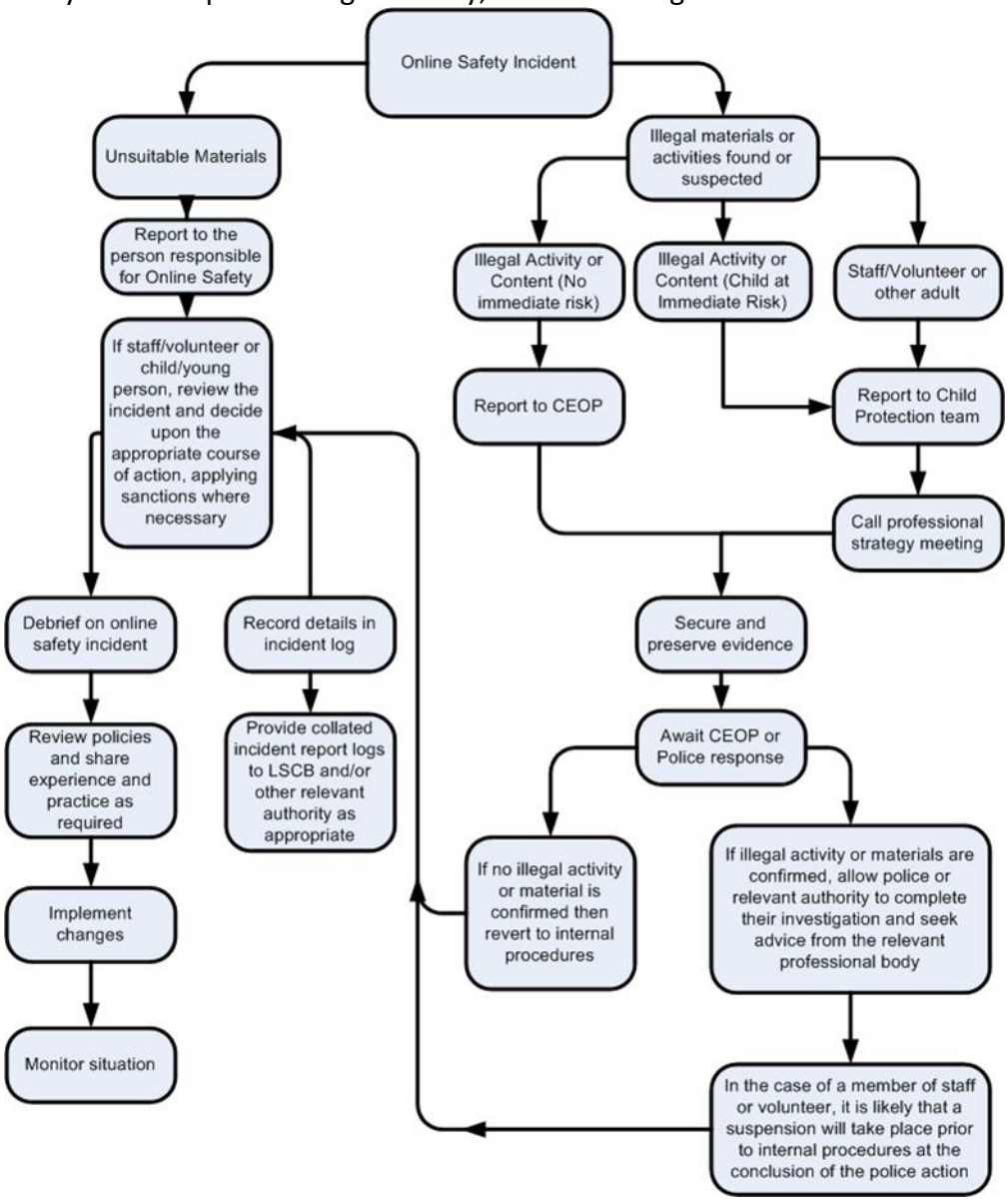
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material,	Child sexual abuse images –The making, production or distribution 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**

remarks, proposals or comments that contain or relate to:	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**	
	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)						
On-line gaming (non educational)						
On-line gambling						
On-line shopping / commerce						
File sharing						
Use of social media						
Use of messaging apps						
Use of video broadcasting eg Youtube						

Responding to incidents of misuse

Illegal Incidents

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



Other Incidents

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

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
- Internal response or discipline procedures
- Involvement by DNEAT, local authority 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
- other criminal conduct, activity or materials including radicalisation
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

Academy Actions & Sanctions

The academy will need to agree sanctions with the Local Governing Body. The academy will need to deal with incidents as soon as possible in a proportionate manner ensuring that members of the academy community are aware that incidents have been dealt with appropriately. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures. (The following responses are to be agreed/amended placing ticks in the appropriate columns **APART FROM Staff**)

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable /		X	X	X					

inappropriate activities).									
Unauthorised use of non-educational sites during lessons									
Unauthorised use of mobile phone / digital camera / other mobile device									
Unauthorised use of social media / messaging apps / 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 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 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:	Refer to line manager	Refer to Headteacher Principal	Refer to DNEAT/ HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning/Management Instruction (informal)	Disciplinary action (formal)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X
Inappropriate personal use of the internet / social media / personal email		X	X				X
Unauthorised downloading or uploading of files		X			X	X	
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account		X	X		X	X	
Careless use of personal data eg	X	X			X	X	

holding or transferring data in an insecure manner							
Deliberate actions to breach data protection or network security rules		X	X	X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X	X			X
Actions which could compromise the staff member's professional standing	X	X				X	
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X	X				X
Using proxy sites or other means to subvert the academy's filtering system		X	X		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X		X	X	
Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X		X
Breaching copyright or licensing regulations		X	X		X	X	
Continued infringements of the above, following previous warnings or sanctions		X	X				X

Signature Date

Headteacher

Signature Date
Chair of Governors

Links to Other Policies

- Data Protection Policy
- Safeguarding Policy
- Bullying and Harassment Policy
- Complaints Policy
- Staff Grievance Procedure
- Disciplinary Procedures
- Statement of procedures for dealing with allegations of abuse against staff
- Code of Conduct

APPENDIX 1

Staff, Governor and Visitor E-Safety and ICT Acceptable Use Agreement

ICT and the related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life in [Academy Name]. This policy is designed to ensure that all adult users are aware of their responsibilities when using any form of ICT. All such users are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with **the Network Manager.**

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for academy business.
- I understand that it is an offence to use the academy's ICT system and equipment for any purpose not permitted by its owner.
- I will only use the academy's email / Internet / Intranet / Learning Platform and any related technologies for uses permitted by the Principal/Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the academy or other related authorities.
- Management may from time to time require access to staff/student data areas, and reserve the right to change passwords/locate data stored in employee's network areas.
- I understand that I am responsible for all activity carried out under my username unless my data has been amended under the direction of the Principal/Headteacher.
- I will ensure that all academy generated electronic communications are appropriate and compatible with my role.
- I will only use the approved, secure email system(s) for any academy business
- I will ensure that all data is kept secure and is used appropriately and as authorised by the
- Principal/Headteacher or Governing Body. If in doubt I will seek clarification. This includes taking data off site.
- I will not browse, download, upload or distribute any material that could be considered

offensive, illegal or discriminatory.

- Images will only be taken, stored and used for purposes in line with academy policy and with written consent of the parent, carer or adult subject. Images will not be distributed outside the academy network/learning platform without the consent of the subject or of the parent/carer, and the permission of the Principal/Headteacher.
- I understand that my permitted use of the Internet and other related network technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal/Headteacher.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding student's safety to the Senior Designated Professional or Principal/Headteacher.
- While [academy Name]'s network administration aims to provide a high level of privacy, users should be aware that the data they create on the corporate systems remains the property of the academy. Because of the need to protect the academy's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the academy. However this does not mean the academy will disclose personal confidential data to third parties.
- Users are not permitted to bring in their own personal laptops and plug into the academy's network.
- Staff must never leave a workstation unattended whilst it is logged on. Lock it by using '*control+alt+delete* and *enter*'.
- Because information contained on portable computers is especially vulnerable, special care should be exercised in looking after them. They should not be left unattended, for example in cars. Sensitive data about children should not be kept on laptop hard drives.
- Data remains the property of [Academy Name], and staff must not disclose personal data pertaining to staff/children to those not authorised to receive it.
- The academy's anti-virus software will automatically delete any files it deems suspicious on external devices such devices as memory pens, so care should be exercised when inserting such devices into a machine.
- In some circumstances employment contracts may expire during academy holidays. However,
- your contract does not entitle you to a laptop. A duty of reasonable care must be taken of laptops and ICT equipment loaned out to staff. This includes not leaving it easily accessible to a thief, or where damage might easily be caused.
- Any cost borne by the academy in replacing/repairing a laptop and/or other device loaned by ICT Where neglect and/or theft/damage has occurred may be passed to the user.
- Laptops left in academy overnight must be in a secure, alarmed area.
- Do not deface your laptop (sticking stickers on it etc.) as it has to be re-allocated when you leave.
- Under no circumstances is an employee of [Academy Name] authorised to engage in any activity that is illegal under national and/or international law while utilising [Academy Name] owned ICT resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.
- The following activities are strictly prohibited:
- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by [Academy Name].

- Circumventing user authentication or security of any machine, network or account.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Staff need to be aware of the implications of using laptops in an uncontrolled environment, i.e. anywhere outside of the academy. To protect the integrity of data on a laptop at home, users should be aware if they allow family members to use the laptop, then the integrity of confidential data is placed at risk. Employees should take all necessary steps to prevent unauthorised access to this information and in doing so comply with the Data Protection Act 1998.
- Under no circumstances must staff contact children via personal e-mail addresses or on commercial social networking sites (e.g. Facebook). They should only use academy based e-mail or the academy's Virtual Learning Environment for such correspondence.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, or other malicious code.
- Postings by employees from an academy e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the academy, unless posting is in the course of business duties.
- Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and the instigation of criminal proceedings. (See Staff Discipline, Conduct and Grievance Policy)

Other relevant policies and information

- Your rights at work; http://www.worksmart.org.uk
- Employment Rights http://www.norfolk.gov.uk
- ICT UK Law http://www.out-law.com
- [Academy Name] Policies and Procedures: Safeguarding; Behaviour; Anti-bullying and Staff Discipline, Conduct and Grievance.
- Data Protection Policy
- Statement of procedures for dealing with allegations of abuse against staff

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the academy.

Full name: ……(PLEASE PRINT)

Job title: …….

Signature: ……

APPENDIX 2

E-Safety and ICT Acceptable Use Rules for children

These e-Safety rules help to protect children and the academy by describing acceptable computer use.

- I understand the academy owns the computer network and learning platform and can set rules for its use.
- I will only use ICT systems in the academy, including the internet, email, digital video, mobile technologies etc, for academy purposes. I can only use it for private purposes with the Principal/Headteacher's permission.
- I will not take photographs or film using a mobile phone.
- I will log on to the academy's network/ learning platform with my own user name and password.
- I accept that I am responsible for all activity carried out under my username.
- I will not use staff computers without permission.
- I will follow the academy's ICT security system and not reveal my passwords to anyone.
- I will make sure that all my ICT communication is responsible, respectful and sensible.
- I will be responsible for my behaviour when using the Internet/learning platform. This includes resources I access, the language I use and the way I look after the equipment.
- I will use the discussion forums on the academy's learning platform for exchanging information and will be constructive in giving my opinions to others.
- I will not give out any personal information about myself or anyone else when using the academy's learning platform.
- If I come across any material that could be considered offensive or illegal I will report it immediately to a teacher.
- I will not download or install software or Apps on academy computers or run any software from any external devices such as memory sticks.
- I will keep within the Internet filtering system and I understand that trying to hack into the system is illegal. I must not bring hacking tools into the academy.
- I will respect the privacy and ownership of others' ICT work at all times.
- I understand the academy may monitor, record and control my use of the academy's computer systems and learning platform.
- During lessons I will only use the computers for academy work.
- I will not eat or drink in the computer rooms/whilst using a computer.
- I understand that these rules are designed to keep me safe and that accept that I will only be allowed to use the academy's equipment and systems by following the rules.
- I understand when I leave [Academy Name] my work will be deleted, and therefore any work I require must be taken with me before I leave.

Rules to be amended/adjusted to match age of pupils within the academy.

Pupil's name: IN CAPITALS LIKE THIS:

_____ _____

F I R S T N A M E L A S T N A M E

Year Group Entering: _____

Pupil's signature: _____ Date: _____

Academy Administration Use Only:

Network Account:
Pupil e-Portal Account:

APPENDIX 3

E-Safety and ICT Acceptable Use Agreement for Parents/Carers

Parent's/Carer's name: _____ (PLEASE PRINT)

Child's name: _____ Year and Class: _____

Child's name:_____ Year and Class: _____

As the parent/carer of the above child(ren), I grant permission for my child(ren) to have access to use the Internet, the Virtual Learning Environment, academy email and other ICT facilities at [Academy Name].

I know that my daughter or son has signed a form to confirm that they will keep to the academy's rules for responsible ICT use, outlined in the e-Safety and ICT Acceptable Use Rules for Children. I also understand that my son/daughter may be informed, if the rules have to be changed during the year. I know that the latest copy of the e-Safety and ICT Acceptable Use Policy and the Rules are available on the 's website insert web address and that further advice about safe use of the Internet can be found through our links on the website.

I accept that ultimately the academy cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the academy will take every reasonable precaution to keep children safe and to prevent children from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-Safety skills to children.

I understand that the academy can check my child's computer files, and the Internet sites they visit. I also know that the academy may contact me if there are concerns about my son/ daughter's e-Safety or e-behaviour.

I will support the academy by promoting safe use of the Internet and digital technology at home and will inform the academy if I have any concerns over my child's e-Safety.

Parent's signature: _____ Date: _____

APPENDIX 4- DfE Guidance on the wording of the Privacy Notice

PRIVACY NOTICE TEMPLATE
for
Pupils in Schools, Alternative Provision and Pupil Referral Units
and Children in Early Years Settings

(This is suggested text which can be amended to suit local needs and circumstances)

Privacy Notice - Data Protection Act 1998

We **(**Name of academy **)** are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school/academy and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your academy is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

In addition for Secondary and Middle deemed Secondary Schools
Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your and your parent's/s' name(s) and address, and any further information relevant to the support services' role. However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service. Please inform *(*Insert name of Academy Administrator*)* if you wish to opt-out of this arrangement. For more information about young peoples' services, please go to the Directgov Young People page at *www.direct.gov.uk/en/YoungPeople/index.htm* .

We will not give information about you to anyone outside the academy without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

(For Academy use only**)** We are required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that we hold and/or share, please contact **(**Insert name of Academy Administrator**).**

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following websites:

[Insert LA website link**]** and

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

[insert details and link to appropriate contact at the LA]

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288