NEW PARK ACADEMY

ONLINE AND MOBILE TECHNOLOGY SAFETY POLICY

FIRST CREATED: MARCH 2010 – EDITION 1

EDITION NO.	REVIEW DATE:	FGB APPROVAL DATE:
		25/6/10
2	NOV 2012	13/11/2012
3	JUNE 2015	24/6/2015
4	SEPTEMBER 2016	
5	JANUARY 2017	02/02/2017
6	SEPTEMBER 2017	19/10/17
7	JANUARY 2018	22/3/18
8	JULY/SEPTEMBER 2018	OCT. 2018
9	JUNE 2020	JULY 2020
10	MARCH 2022	NO CHANGES
11	MARCH 2023	NO CHANGES
12	MARCH 2024	NO CHANGES

Policy Agreed	**VIA EMAIL JULY 2020**
To be reviewed	**MARCH 2025**
Owner	**JANE KING**
Signed	
Designation	**IT HEAD**

Vision Statement and Ethos

Nurture

Our dedicated, motivated and well trained staff create a caring and safe environment where the needs of every young person is addressed and where every child is supported and encouraged to excel.

Equality

Everyone in our academy is valued equally, whatever their roles, abilities, beliefs, sexual preferences or needs are. We believe every individual is special and their unique qualities are recognised and celebrated in our academy.

Well-being

We strive to ensure that the physical, emotional, academic and mental health needs of all members of our academy community are met, and to do this we rely on the support our pupils' families, carers and a range of external agencies.

Progress

New Park offers a broad, creative and therapeutic curriculum which supports our pupils learning and nourishes their emotional growth. At each stage in their learning, our pupils are supported and nurtured allowing them to fulfil their potential in every area.

Achievement

Through commitment and dedication to their studies, our students acquire the knowledge, skills and independence needed to help them adapt to the different challenges that they will face in academy and in life's journey, and support them as they move towards achieving their personal and academic goals.

Reward

We recognise and celebrate each individual pupil's achievement in learning and behaviour and the many contributions they make to the academy community.

Knowledge

We support our young people to gain the knowledge, skills and understanding to help them on their journey through academy and beyond.

Policy Governance

Development, Monitoring and Review of this Policy

This online and mobile technology safety policy has been developed by the CS coordinator Jane King in cooperation with the IT technician in consultation with the Headteacher, based on Salford's model policy.

Position	Name(s)
Academy Online and mobile technology safety Coordinator / Officer	Jane King
Headteacher	Almut Bever-Warren
ICT Technical staff	Katie Green
Governors	Yvonne Luckin

Consultation with the whole academy community has taken place through the following:

Forum	Date (if applicable)
Staff meetings	Ongoing agenda item
Academy / Student / Pupil Council	On-going through taught sessions
Governors meeting	Permanent agenda item
Academy website / newsletters	Current up to date policy displayed on website.

Schedule for Review

This online and mobile technology safety policy was approved by the *Governing Board* on:	JULY 2020
The implementation of this online and mobile technology safety policy will be monitored by:	Online and mobile technology safety Coordinator Jane King
Monitoring will take place at regular intervals:	Annually
The *Governing Board* will receive a report on the implementation of the online and mobile technology safety policy generated by the Online and mobile technology safety Coordinator Jane King at regular intervals:	In the autumn term report
The Online and mobile technology safety Policy will be reviewed *annually*, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online and mobile technology safety or incidents that have taken place. The next anticipated review date will be:	MARCH 2025
Should serious online and mobile technology safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager: Terry Walsh CEO: Bev Walker Data Protection Officer: Dilys Morgan (0161 912 3082) LADO Police Commissioner's Office

Due to changes in educational landscape since Covid 19, rapid changes have been facilitated in regards to online learning so we have updated this policy in line with the requirements.

The academy will monitor the impact of the policy using:

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

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-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.

Roles and Responsibilities

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

Advisory Board:

- Advisors are responsible for the approval of the Online and Mobile Technology Safety Policy and for reviewing the effectiveness of the policy.

This will be carried out by the Advisors receiving regular information about online safety incidents and monitoring reports. A member of the Advisory Board has taken on the role of Online Safety Advisor (it is suggested that the role may be combined with that of the Child Protection/Safeguarding Advisor). The role of the Online Safety Advisor will include:

- meetings with the Online Safety Co-ordinator/officer
- attendance at Online Safety Group meetings
- monitoring of online safety incident logs
- monitoring of filtering/change control logs
- reporting to relevant Advisor meeting

Headteacher and Senior Leaders:

- The Headteacher 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 Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority/MAT/other relevant body disciplinary procedures).
- The Headteacher/Principal and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in academy who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online and mobile technology safety Coordinator/Officer:

Jane King leads the online and mobile technology safety committee and/or cross-academy initiative on online and mobile technology safety, supported by the IT Technician.

- 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 staff 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 staff
- liaises with the Local Authority/MAT/relevant body
- liaises with academy technical staff
- receives notice of online safety incidents and log of incidents from the Headteacher to inform future online safety developments.
- meets with Online Safety Advisor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of the Advisory Board
- reports to Senior Leadership Team

Network Manager / Technical staff:

The Network Manager is responsible for ensuring:

- that the academy's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the academy meets the online and mobile technology safety technical requirements outlined in the Salford City Council Security Policy and

Acceptable Usage Policy and any relevant Local Authority Online and mobile technology safety Policy and Staff Laptop and Portable Electronic Device Policy guidance as well as the Sovereign Trust Security Policies

- that users may only access the academy's networks through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/Principal and Senior Leaders; Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in academy/academy policies
-

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online and mobile technology safety matters and of the current academy online and mobile technology safety policy and practices
- they have read, understood and signed the academy Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the online and mobile technology safety Co-ordinator 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
- online safety issues are embedded in all aspects of the curriculum and other activities
- students/pupils understand and follow the Online Safety Policy and acceptable use policies
- students/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 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

Designated person for child protection/Child Protection Officer, Almut Bever-Warren, endeavours to be trained in online and mobile technology safety issues and be aware of the potential for serious Child Protection issues to arise from:

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

- cyber-bullying
- extremist materials exhibiting any of the following:
  vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs; and/or calls for the death of members of our armed forces, whether in this country or overseas (refer to Prevent Policy).

Online and mobile technology Safety Committee

The committee provides a consultative group that has wide representation from the academy community, with responsibility for issues regarding online safety and the monitoring the Online and Mobile Technology Safety Policy including the impact of initiatives. Depending on the size or structure of the academy this group may be part of the safeguarding group. The group will also be responsible for regular reporting to the Advisory Board.

Members of the Online and Mobile Technology Safety Committee will assist the Online and mobile technology safety Coordinator with:

- the production, review and monitoring of the academy online and mobile technology safety policy
- 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 online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the students/pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Students/pupils:

- are responsible for using the academy ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to academy systems need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 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 online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of academy and realise that the academy's/academy's online safety policy covers their actions out of academy, if related to their membership of the academy.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local online and mobile technology safety campaigns/literature.

Parents and carers will be encouraged to support the academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at academy events

- access to parents' sections of the website/Learning Platform and on-line student/pupil records

- their children's personal devices in the academy (where this is allowed)

Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the academy ICT systems or Learning Platform in accordance with the academy Acceptable Use Policy.

Community Users

Community Users who access academy ICT systems or Learning Platform as part of the Extended Academy provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to academy systems.

Online and mobile technology safety Education and Training

Education – students / 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/digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online 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 supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. N.B. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material 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 school/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, 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 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 and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. 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 online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The academy website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool for groups such as these - www.onlinecompass.org.uk

Education & Training – Staff

It is essential that all staff receive online and mobile technology 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 staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events (e.g. from LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Education and Training – Advisors

Advisors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation.

- Participation in academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

The school/academy is responsible for ensuring that the school/academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities: **School/academy technical systems will be managed in ways that ensure that the school/academy meets recommended technical requirements**

- **There will be regular reviews and audits of the safety and security of school/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 school/academy technical systems and devices.**
- **All users will be provided with a username and secure password by** the IT Technician *who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password**.
- The IT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users.** Illegal content (child sexual abuse images) is filtered by the broadband 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. There is a clear process in place to deal with requests for filtering changes.
- **Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.**
- *The school/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)
- *School/academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.*

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.*
- *An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place*) *regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices.* ***Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured***.

Mobile Technologies (including BYOD/BYOT)

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

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s online safety education programme.

- **The school acceptable use agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies**
- **The school allows:**

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*		*Yes*		*Yes*	
Internet only		*Yes*				*Yes*
No network access				*Yes*		

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students/pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students/pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- **When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.**
- **Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website/social media/local press**
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.

- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school/academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that students/pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
- Students/pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Student's/Pupil's work can only be published with the permission of the student/pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school/academy must ensure that:

- **it has a Data Protection Policy.**
- **it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.**
- **it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).**
- **it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.** The school/academy may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- **it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it**
- **the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded**
- **it will hold only 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. The school should develop and implement a 'retention**

policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- **it provides staff, parents, volunteers, teenagers and older children with information about how the school/academy looks after their data and what their rights are in a clear Privacy Notice procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).**
- **data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)**
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- **it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.**
- **it understands how to share data lawfully and safely with other relevant data controllers.**
- **it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.**
- **If a maintained school/academy, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.**
- **all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.**

When personal data is stored on any mobile device or removable media the:

- **data must be encrypted and password protected.**
- **devices must be password protected.**
- **device must be protected by up to date virus and malware checking software**

- **data must be securely deleted from the device, in line with school/academy policy (below) once it has been transferred or its use is complete.**

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**
- **can recognise a possible breach, understand the need for urgency and know who to report it to within the school**
- **can help data subjects understands their rights and know how to handle a request whether verbal or written and know who to pass it to in the school**
- **where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.**
- **will not transfer any school/academy personal data to personal devices except as in line with school policy**
- **access personal data sources and records 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**

Communications

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

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

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students/Pupils**
Mobile phones may be brought to academy	Yes, but must be locked away in personal locker in staff room unless special permission has been sought by SLT	Yes but academy does not take any responsibility for the phone, and it must not be used during lesson
Use of mobile phones in lessons	No – unless there is a very specific reason which has been cleared with SLT eg: ICT lesson	No - unless there is a very specific reason which has been cleared with staff eg: ICT lesson
Use of mobile phones in social time	After academy	no
Taking photos on personal mobile phones or other camera devices	With permission of SLT and parents during special events/trips	Under direction of staff, and with permission of students
Use of personal hand held devices e.g. PDAs, PSPs	If part of a lesson	If part of a lesson
Use of personal email addresses in academy, or on academy network	No – apart from before or after academy	No
Use of academy email for personal emails	Work email should not be used for private business	no
Use of chat rooms / facilities	no	no
Use of instant messaging	no	no
Use of social networking sites	Only before or after academy	no
Use of blogs	Only if part of a academy project	Only if part of a academy project

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

- **The official *school/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 school/academy email service to communicate with others when in school, or on school/academy systems (e.g. by remote access).*

- **Users must immediately report, to the nominated person – in accordance with the school/academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Any digital communication between staff and students/pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school/ academy systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Whole class/group email addresses may be used at KS1, while students/pupils at KS2 and above will be provided with individual school/ academy email addresses for educational use.*
- *Students/pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.*
- *Personal information should not be posted on the school/ academy website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

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

The school/academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School/academy staff should ensure that:

- No reference should be made in social media to students/pupils, parents/carers or school/academy staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school /academy* or local authority/MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school/academy social media accounts are established there should be:

- *A process for approval by senior leaders*
- *Clear processes for the administration and monitoring of these accounts – involving at least two members of staff*
- *A code of behaviour for users of the accounts, including*
- *Systems for reporting and dealing with abuse and misuse*
- *Understanding of how incidents may be dealt with under school/academy disciplinary procedures*

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school/academy or impacts on the school/ academy, it must be made clear that the member of staff is not communicating on behalf of the school/academy with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- *The school/academy permits reasonable and appropriate access to private social media sites*

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

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

Dealing with unsuitable/inappropriate activities

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

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

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions	☑	⚠	⚠	☒	☒
Child sexual abuse images					☒
Promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☒
Adult material that potentially breaches the Obscene Publications Act in the UK					☒
Criminally racist material in UK Extremist or Terrorism related material					☒
Pornography					☒
Promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
Promotion of racial or religious hatred					☒
Threatening behaviour, including promotion of physical violence or mental harm					☒
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute				☒	
Using academy systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the academy				☒	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				☒	
Creating or propagating computer viruses or other harmful files				☒	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes				☒	

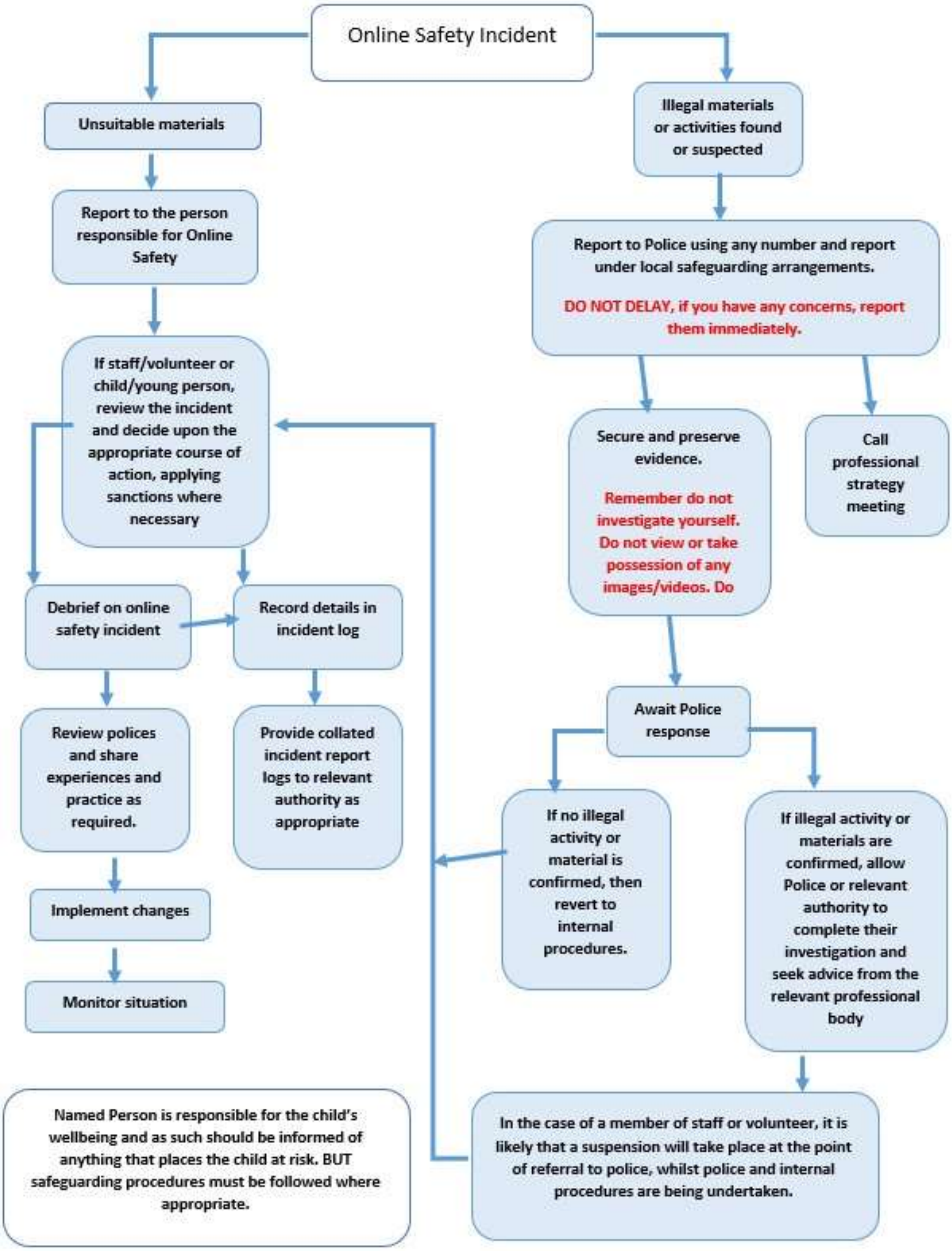
network congestion and hinders others in their use of the internet					
On-line gaming (educational)		⚠			
On-line gaming (non educational)		⚠			
On-line gambling				☒	
On-line shopping / commerce		⚠			
File sharing		⚠			
Use of social networking sites		⚠			
Use of video broadcasting e.g. YouTube			⚠		
Accessing the internet for personal or social use (e.g. online shopping)		⚠			
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses				☒	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart below for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

Good practice guidelines

Email

Best practice

☑ **DO**

Staff and students/pupils should only use their academy email account to communicate with each other

Safe practice

⚠

Check the academy online and mobile technology safety policy regarding use of your academy email or the internet for personal use e.g. opping

Poor practice

☒ **DO NOT**

Staff: don’t use your personal email account to communicate with students/pupils and their families without a manager’s knowledge or permission – and in accordance with the online and mobile technology safety policy.

Images, photos and videos

Best practice

☑ **DO**

Only use academy equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

⚠

Check the online and mobile technology safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the academy network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ **DO NOT**

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the online and mobile technology safety policy.

Don’t retain, copy or distribute images for your personal use.

Internet

Best practice

☑ **DO**

Understand how to search safely online and how to report inappropriate content.

Safe practice

⚠

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the online and mobile technology safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ **DO**

Staff: If you need to use a mobile phone while on academy business (trips etc), the academy may ask you to use your own phone to contact the office staff or SLT. However, you should not use your own phone to contact parents or children. If you need to be in contact with parents on a regular basis, academy will supply you with a work mobile.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

⚠

Check the online and mobile technology safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ DO NOT

Staff: Don’t use your own phone without the Headteacher/SLT knowledge or permission.

Don’t retain service student/pupil/parental contact details for your personal use.

Social networking (e.g. Facebook/ Twitter)

Best practice

☑ DO

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends to not post tagged images of you on their open access profiles.

Safe practice

⚠

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ **DO NOT**

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

⚠

Check the online and mobile technology safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the academy network immediately after the event.

Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

Don’t download images from organisation equipment to your own equipment.

Don’t use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the online and mobile technology safety policy.

Don’t retain, copy or distribute images for your personal use.

Incidents (students/pupils):	Refer to class teacher	Refer to Headteacher	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 e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X						X	
Unauthorised use of mobile phone/digital camera / other handheld device	X				X		X	X
Unauthorised use of social networking/ instant messaging/personal email		X			X	X		X
Unauthorised downloading or uploading of files		X		X	X	X		
Allowing others to access academy network by sharing username and passwords	X			X	X	X		
Attempting to access or accessing the academy network, using another student's/pupil's account	X			X		X	X	
Attempting to access or accessing the academy network, using the account of a member of staff		X			X	X		X
Corrupting or destroying the data of other users		X		X	X	X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X		X	X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X	X	X		X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy		X		X	X	X		X
Using proxy sites or other means to subvert the academy's filtering system		X		X	X	X		X

Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X	X	X		X
Deliberately accessing or trying to access offensive or pornography		X	X	X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X	X	X	X	X
Accidentally accessing Extremist or Terrorism related material		X	X	X	X	X	X	X
Deliberately accessing Extremist or Terrorism related material		X	X	X	X	X	X	X

Incidents (staff and community users): *(Any of the below inappropriate actions may lead to further disciplinary investigations, particularly if there have been previous concerns)*	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction : disciplinary hearing
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	x
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / 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	
Careless use of personal data e.g. holding or transferring data in an insecure manner	x		x		x	
Deliberate actions to breach data protection or network security rules	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 instant 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	
Actions which could compromise the staff member's professional standing	x		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	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	(x)	x		x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x			x
Breaching copyright or licensing regulations	x		x		x	
Continued infringements of the above, following previous warnings or sanctions	x		x	x		x
Accidentally accessing Extremist or Terrorism related material	x	(x)	x		x	x
Deliberately accessing Extremist or Terrorism related material	x	x	x			x

Further information and support
For a glossary of terms used in this document:
http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

For online and mobile technology safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:
http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf
R u cyber safe?
Online and mobile technology safety tips about how to stay safe online:
http://www.salford.gov.uk/rucybersafe.htm

Appendix 1 – Student/Pupil AUP

Student/pupil Acceptable Use Policy Agreement Template

Student/Pupil Acceptable Use Policy Agreement

This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The academy will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.

☑ I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change any one else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- only use my personal handheld/external devices (mobile phones/USB devices etc) in academy if I have permission
- understand that, if I do use my own devices in academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment
- Understand that academy will not pay for damage to or loss of any equipment I choose to bring to academy
- immediately report any damage or faults involving equipment or software, however this may have happened
- do not use chat and social networking sites

☒ I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the academy ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings

Student / Pupil Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions, both in and out of academy:

- I understand that the academy also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of academy and where they involve my membership of the academy community (examples would be cyber-bullying, use of images or personal information)

- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may loss of access to the academy network/internet, detentions, fixed term exclusions, contact with parents and in the event of illegal activities involvement of the police

I have read and understand the above and agree to follow these guidelines when:

- I use the academy ICT systems and equipment (both in and out of academy)

- I use my own equipment in academy (when allowed) e.g. mobile phones, PDAs, cameras etc

- I use my own equipment out of academy in a way that is related to me being a member of this academy e.g. communicating with other members of the academy, accessing academy email, Learning Platform, website etc

(Parents/carers are requested to sign the permission form below to show your support of the academy in this important aspect of the academy's work).

Name of Student/Pupil		
Signed (Student/Pupil)		Date
Signed (Parent/Carer)		Date

Appendix 2 – Staff, Volunteer, Community User AUP

Staff, Volunteer and Community User Acceptable Use Policy Agreement

Academy Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The academy will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online and mobile technology safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of academy ICT systems (e.g. laptops, email, VLE etc) out of academy

- I understand that the academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the academy

- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using academy ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the academy website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use chat and social networking sites in academy in accordance with the academy's policies.

- I will only communicate with students/pupils and parents/carers using official academy systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

The academy and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules in line with the Academy's Online and mobile technology safety Policy set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.

- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies

- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Academy/Local Authority Personal Data Policy). Where personal data is transferred outside the secure academy network, it must be encrypted.

- I understand that data protection policy requires that any staff or student / pupil data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy ICT equipment in academy, but also applies to my use of academy ICT systems and equipment out of academy and my use of personal equipment in academy or in situations related to my employment by the academy.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a disciplinary hearing including suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police

  - **I have read and understood the Academy's Online and mobile technology safety Policy**

I have read and understand the above and agree to use the academy ICT systems (both in and out of academy) and my own devices (in academy and when carrying out communications related to the academy) within these guidelines.

Name	
Position	
Signed	
Date	

Appendix 3 – Use of Images Consent Form

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Students/Pupils and members of staff may be using digital or video 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,
The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the academy to take and use images of their children.

Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above student / pupil, I agree to the academy taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the academy.

I agree that if I take digital or video images at, or of, academy events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	