Diocese of Norwich Education and Academies Trust

Diocese of Norwich St Benet's Multi Academy Trust

Open Academy

Online Policy

Policy Type:	**Trust Policy**
Date Issued by MAT:	**04/05/2023**
Approved By:	**Trust Board (Joint Policy Development Committee)**
Approval Date:	**09/03/2023**
Review Date:	**March 2024**
Person Responsible:	**Head of Safeguarding**

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
5	Schedule for monitoring and review	Clarification of online safety lead role may form part of DSL or Business Manager role and may be part of DSL meetings. Updated list of external reporting bodies	Feb 21
14	Technical – infrastructure / equipment, filtering and monitoring	Use of mobile data management system Use of Trend AV across the Trust	Sep 21 Feb 22
17	Data Protection	Updated in line with UK Data Protection laws to included personal data stored on mobile devices/removable media	Feb 21
18	Data Protection	Staff section updated to include recognition of possible breach	Feb 21
22	Unsuitable/inappropriate activities	Table updated to include Computer Misuse Act	Feb 21
24	Illegal incidents	Flow chart updated	Feb 21
28	Links to Other Policies	Updated Safeguarding Policy 2022	Feb 23
	Throughout	E-safety renamed online safety in line with Dfe guidance	Nov 21
53	DNEAT/ RM Unify Password Policy	Addition of DNEAT/ RM Unify Password Policy Appendix 9 DNEAT ACADEMIES ONLY	May 21
16	Data Protection	FOI requests and SARs to be sent to Head of Human Resources via GDPR-HR@donesc.org	March 23
18	Social Media - Protecting Professional Identity	Employee Social Media profiles to be set to private and not public	March 23

Table of Contents

Our Christian Ethos and Values
All policies within the Diocese of Norwich Education and Academies Trust (hereafter referred to as "the Trust"), whether relating to an individual academy or the whole Trust, will be written and implemented in line with our Christian ethos and values.

> **DNEAT**: We make no apologies for having high ambition for all, and we truly value the wider educational experience.
> We walk and talk our Christian values. That means we put people at the centre of the organisation and want to see them flourish and grow. Our schools are inclusive, welcoming those of all faiths and none.

Overall accountabilities and roles
The Trust has overall accountability for all its academies and staff. Through a Scheme of Delegation for each academy it sets out the responsibilities of the Trust, its Executive Officers, the Local Governing Body and the Principal. The Principal / Head Teacher of each academy is responsible for the implementation of all policies of the Trust.
All employees of the Trust are subject to the Trust's policies.

Open Academy has an overview of online safety.
Our Online Safety Policy is based on national educational trust guidelines. It has been agreed by the Leadership Team and noted by the Local Governing Body.

Schedule for Development/Monitoring/Review
The implementation of this Online policy will be monitored by the Safeguarding and Health and Safety Lead Officer (DoNESC Head of Estates)/ LGB/ Safeguarding Governor (Nick Plater)

Monitoring will take place at regular intervals.

The Trustees/LGB will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents annually.

The online 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 safety or incidents that have taken place.

Should serious online safety incidents take place, the following external persons/agencies be informed (Trust Safeguarding Lead & Health and Safety Lead (DoNESC Head of Estates) & Data Protection Officer/ Police/ ICT Network team/ICT Solutions)

The academy will monitor the impact of the policy using

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

-Staff

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

The Education and Inspections Act (2006) empowers Principals to such an extent as is reasonable, to regulate the behaviour of students when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy and the Trust. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (See Appendix 7). 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 online safety behaviour that take place out of the academy.

Roles and Responsibilities
The Board of Trustees are responsible for the approval of the online safety policy. The LGB are responsible for monitoring the implementation of this policy. This will be carried out by the Trustees/LGB receiving regular information about online safety incidents and monitoring reports. A member of the LGB has taken on the role of online safety Governor and the role includes:

- regular meetings with the online safety Co-ordinator/Officer – this may form part of the Designated Safeguarding Lead role and/or Business Manager
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant LGB/Trust Board/Committee/ meeting

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day-to-day responsibility for online safety will be delegated to the online safety lead.
- The Principal 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 online safety allegation being made against a member of staff
- The Principal/Senior Leaders are responsible for ensuring that the online safety Coordinator/Officer 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 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 online 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 online safety Lead

Online safety lead

- Leads the online safety (this may be combined with Child Protection/Safeguarding Officer role and the DSL meetings)
- Takes day to day responsibility for online safety issues and has a leading role in establishing and review 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 Trust Safeguarding Lead/ relevant body
- Liaises with academy technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with online 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 online safety measures as outlined below and that the managed service provider is fully aware of the academy online 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 online safety technical requirements and any Trust / other relevant body Online safety Policy / Guidance that may apply.
- That users may only access the networks and devices 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 person
- 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 network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Senior Leader; Online safety Coordinator / Officer 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 online safety matters and of the current academy online 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 Principal / Senior Leader; Online safety Coordinator / Officer for investigation / action / sanction
- All digital communications with students / 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 understand and follow the online safety and acceptable use policies
- 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 students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead / Child Protection Officer
Should be trained in online 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 online safety Officer with Safeguarding role

Online safety responsible person
The Online safety person provides a consultative gr that has wide representation from the academy community, with responsibility for issues regarding online safety and the monitoring the online safety policy including the impact of initiatives. Depending on the size or structure of the academy this may be part of the DSL safeguarding group within the school. The group will also be responsible for regular reporting to the LGB and then to the Trust Board.

The online responsible person will assist the Online safety Coordinator / Officer (or other relevant person, as above) with:

- The production / review / monitoring of the academy online 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 online safety digital literacy curricular provision – ensuring relevance, breadth and progression
- Monitoring network / internet / incident logs
- Consulting stakeholders – including parents / carers and the students about the online safety provision
- Monitoring improvement actions identified

Students:

- Are responsible for using the academy digital technology systems in accordance with the Student Acceptable Use Agreement
- 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 online safety practice when using digital technologies out of academy and realise that the academy's Online 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 online 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 (see Use of Digital Images and Videos policy guidelines below)
- access to parents' sections of the website / VLE and on-line student records
- their children's personal devices in the academy (where this is allowed)

Community Users

Community Users who access academy systems/website/Learning platform as part of the wider academy provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access to academy systems (See appendix 6)

Policy Statements

Education – students

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

Online safety should be a focus in all areas of the curriculum and 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 should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students 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.
- Students should be helped to understand the need for the student 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 should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, 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 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 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:

- 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 ThinkUknow

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:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- 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
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their online safety provision

Education & Training – Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. It is expected that some staff will identify online safety as a training need within the performance management process.
- 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.
- The Online safety Coordinator / Officer will receive regular updates through attendance at external training events 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 / INSET days.
- The Online safety Coordinator / Officer will provide advice / guidance / training to individuals as required.

Training – Governors

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

- Attendance at training provided by the Trust/NGA / National Governors Association / or other relevant organisation.
- Participation in academy training / information sessions for staff or parents.

Use of Digital Imaging Technologies

The development of digital imaging technologies has created significant benefits to learning allowing staff and students instant use of images that they have recorded themselves of or downloaded from the internet. Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the public media, However, staff, parents, carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The academy will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students are published on the academy 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 academy events for their own personal use (as such use in not covered by the General Data Protection Regulations). 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 students in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

Students must not take, use, share, publish or distribute images of others without their permission

Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Student's work can only be published with the permission of the student and parents or carers.

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
For those academies using the Trust managed ICT service provider RM Unify or ERGO, they undertake to ensure all relevant online safety measures are in place around network, cloud hosting and infrastructure. The Trust will ensure the managed ICT service provider is fully aware of the Trust-wide online safety and acceptable use of ICT policy and agreements. Password control will be in line with the Trust and ICT Service provider password policy (Appendix 9).
Trend AV is deployed across the Trust's devices. Each machine that is enrolled into the Intune system has Trend installed automatically. Trend will automatically get any AV package updates direct from Trend as soon as they are released and will install without input from the user. The

machine themselves are also set to connect to Microsoft to check for updates and if any are found these are downloaded and also installed without input from the user.

Trust owned mobile devices are required to be kept up to date with vendor updates and app patches. The Trust will use mobile device management tools to ensure enforcement and control.

Otherwise:
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 online safety responsibilities:

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements (these may be outlined in Trust wide/ 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 three months. (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 Principal or other nominated senior leader and kept in a secure place (e.g. academy safe)
- The IT technician in conjunction with ICT solutions 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. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The academy has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different ages / stages and different groups of users – staff / 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.

- An appropriate system is in place using a dedicated email address for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- 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 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 utilising a dedicated email address and log in 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 regarding the extent of personal use that users (staff / students / 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 that forbids staff from downloading executable files and installing programmes on academy devices.
- An agreed policy is in place that encrypts removable media on insertion to academy devices 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 (refer to Trust wide Data Protection &FOI Policy).

Mobile Technologies (including Bring Your Own Device BYOD/ Technology BYOT)
Mobile technology devices may be academy owned/provided or personally owned and and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the academy's wireless network. The device then has access to the wider internet which may include the academy'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 academy context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant academy polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Data Protection & FOI 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 academy's Online Safety education programme.

- The academy Acceptable Use Agreements for staff, students and parents/carers gives consideration to the use of mobile technologies
- The academy allows**:**

	Academy Devices	Personal Devices

	Academy owned for single user	Academy owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in academy	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only			*Yes*	*No* *Caveat for KS5 learners*	*Yes*	*Yes*
No network access						

- The academy has a set of clear expectations and responsibilities for all users
- The academy adheres to the General Data Protection Regulation 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 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

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

The Trust must ensure that:

- It has paid the appropriate fee to the Information Commissioner's Office (ICO).
- It has appointed a Data Protection Officer (DPO) who has a high level of understanding of data protection laws and is free from any conflict of interest.
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, privacy notices and records.

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

The academy must ensure that:

- It implements the data protection principles and is able to demonstrate that it does so through use of policies,
- privacy notices and records.
- 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. It follows the Trust Data Protection and 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. It must 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 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.
- FOI requests and Subject Access Requests are to be sent to the Trust Data Protection Officer, Jo Leach, Head of Human Resources via GDPR-HR@donesc.org.
- 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.

- device must be password protected. (be sure to select devices that can be protected in this way)
- 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. 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 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

This is an area of rapidly developing technologies and uses. Academy's will need to discuss and agree how they intend to implement and use these technologies e.g. some academy's do not allow students to use mobile phones in lessons, while others recognise their educational potential and allow their use. This section may also be influenced by the age of the students.

	Staff and other adults			Student / pupils				
COMMUNICATION TECHNOLOGIES	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed - Staff	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed – Students
Mobile Phones may be brought into the academy	X				X			
Use of mobile phones in lessons							X	
Use of mobile phones in social time	X							X

Taking photos on mobile phones / cameras			X					X
Use of other mobile devices e.g. tablets, gaming devices		X						X
Use of personal email addresses in academy, or on academy network	X							X
Use of academy email for personal emails				X			X	
Use of messaging apps	X							X
Use of social media		X						X
Use of blogs	X						X	

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 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 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 at KS2 and above will be provided with individual academy email addresses for educational use.
- Students 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 academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All MATs, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. MATs, 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 the Trust 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 students, staff and the academy through:

- Ensuring that personal information is not published
- Social media profiles are set to private and not public.
- 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 Trust staff should ensure that:
- No reference should be made in social media to students, 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 the Trust
- 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 online safety committee to ensure compliance with the Social Media, Data Protection, Communications policies and Online safety and ICT Acceptable Use Policy

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 academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the 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 academy are outside the scope of this policy
- Where excessive personal use of social media in academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The academy permits reasonable and appropriate access to private social media sites at the discretion of the Principal

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 academy and the Trust
- The academy should effectively respond to social media comments made by others according to a defined policy or process

The academy's use of social media for professional purposes will be checked regularly by the Trust and Online Safety Group to ensure compliance with the academy policies.

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:

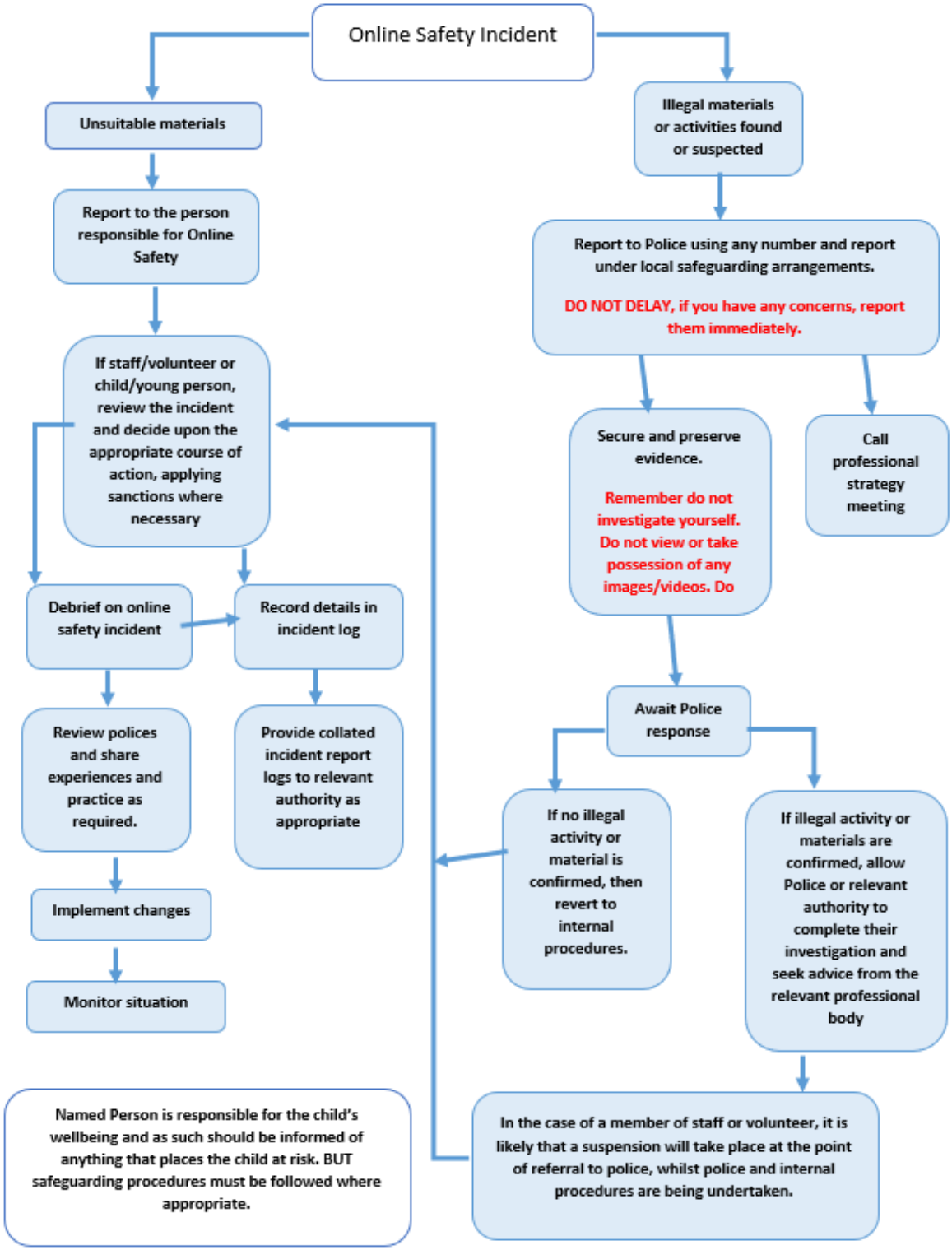
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					**X**
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					**X**
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					**X**
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					**X**
	pornography					**X**
	promotion of any kind of discrimination				**X**	
	threatening behaviour, including promotion of physical violence or mental harm					**X**
	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**	
	Promotion of extremism or terrorism					**X**
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute				**X**	

	Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					**X**
Using academy systems to run a private business					**X**	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy					**X**	
Infringing copyright					**X**	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					**X**	
Creating or propagating computer viruses or other harmful files					**X**	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					**X**	
On-line gaming (educational)					**X**	
On-line gaming (non educational)					**X**	
On-line gambling					**X**	
On-line shopping / commerce					**X**	
File sharing					**X**	
Use of social media					**X**	
Use of messaging apps					**X**	
Use of video broadcasting eg Youtube					**X**	

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 to online safety incidents and report immediately to the police.



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 the Trust, 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
- promotion of terrorism or extremism
- 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.

Students **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 / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons								x	x
Unauthorised use of mobile phone / digital camera / other mobile device								x	x
Unauthorised use of social media / messaging apps / personal email								x	x
Unauthorised downloading or uploading of files							x	x	x
Allowing others to access academy network by sharing username and passwords							x	x	x
Attempting to access or accessing the academy network, using another student's account							x	x	x
Attempting to access or accessing the academy network, using the account of a member of staff							x		x
Corrupting or destroying the data of other users							x		x
Sending an email, text or message that is regarded as						x	x		x

offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions							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
Accidentally accessing offensive or pornographic material and failing to report the incident								x	x
Deliberately accessing or trying to access offensive or pornographic material						x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the GDPR								x	x

Staff

Incidents:	Refer to line manager	Refer to Headteacher Principal	Refer to Trust/ 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 holding or transferring data in an insecure manner	X	X			X	X	
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		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
Principal

Signature Date
Chair of Governors

Links to Other Policies

- Data Protection & FOI Policy
- Safeguarding Policy 2022
- 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
- Preventing Extremism and Radicalisation Policy

APPENDIX 1: Staff (and Volunteer) Online safety and ICT Acceptable Use Agreement

Open Academy

New technologies have become integral to the lives of children and young people in today's society, both within academy's / academies and in their lives outside academy. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

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

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that the academy will monitor my use of the academy digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of academy, and to the transfer of personal data (digital or paper based) out of academy.
- I understand that the academy digital technology 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 (eg 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 social networking sites in academy in accordance with the academy's policies.
- I will only communicate with students 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 Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:
- When I use my mobile devices (laptops / tablets / 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 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 use personal email addresses on the academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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 Trust Data Protection & FOI Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student 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).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment in academy, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises 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 suspension, referral to the Trust or the Local Authority and in the event of illegal activities the involvement of the police.
- I have read and understand the above and agree to use the academy digital technology 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.

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: Online 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 Open Academy.

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 online 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 online safety and ICT Acceptable Use Policy and the Rules are available on the academy's website open-academy.org.uk 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 online 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 online 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 online safety.

Parent's signature: _____ Date: _____

APPENDIX 3: Use of Cloud Systems Permissions Form

The academy uses Microsoft Cloud Based Apps (Office 365) for Education for students and staff. This permission form describes the tools and student responsibilities for using these services.

The following services are available to each student and hosted by Microsoft as part of the academy's online presence in Microsoft Office 365 for Education:

Mail/Calendar - an individual email account for academy use managed by the academy

Microsoft Teams - an individual calendar providing the ability to organize schedules, daily activities, and assignments

Microsoft Office suite - a word processing, spreadsheet, drawing, and presentation toolset

Microsoft Sway - an individual and collaborative website creation tool

Using these tools, students collaboratively create, edit and share files and websites for academy related projects and communicate via email with other students and members of staff. These services are entirely online and available 24/7 from any Internet-connected computer. Examples of student use include showcasing class projects, building an electronic portfolio of academy learning experiences, and working in small groups on presentations to share with others.

The academy believes that use of the tools significantly adds to your child's educational experience.

As the parent / carer of the above student, I agree to my child using Microsoft 365.	Yes / No

Signed: .....

Date: .....

APPENDIX 4: Acceptable use template for older students

Academy Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.
This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement
I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.
For my own personal safety:

- I understand that the academy will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that everyone has equal rights to use technology as a resource and:
- I understand that the school / academy systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the academy systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so. (schools / academies should amend this section to take account of their policy on each of these issues)

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will 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.
- I will not take or distribute images of anyone without their permission.
- I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school / academy:
- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission (academies should amend this section in the light of their mobile devices policies). I understand that, if I do use my own devices in the school / academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed (schools / academies should amend this section to take account of their policy on access to social media).
- When using the internet for research or recreation, I recognise that:
- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I understand that I am responsible for my actions, both in and out of school:
- 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 school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include (academies should amend this section to provide relevant sanctions as per their behaviour policies) loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached.
Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems. (academies will need to decide if they require students to sign, or whether they wish to simply make them aware through education programmes / awareness raising).
I have read and understand the above and agree to follow these guidelines when:

- I use the school / academy systems and devices (both in and out of school)
- I use my own devices in the school / academy (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school / academy in a way that is related to me being a member of this school / academy e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student:

Group / Class:

Signed:

Date:

Parent / Carer Countersignature (optional)

It is for academies to decide whether or not they require parents / carers to sign the Parent / Carer Acceptable Use Agreement This includes a number of other permission forms (including digital and video images / biometric permission / cloud computing permission).
Some academies may, instead, wish to add a countersignature box for parents / carers to this student Acceptable Use Agreement.

APPENDIX 5: Student Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

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

Signed (child):

Signed (parent):

Primary schools using this acceptable use agreement for younger children may also wish to use (or adapt for use) the Parent / Carer Acceptable Use Agreement as this provides additional permission forms (including the digital and video images permission form).

Appendix 6: Community Users Acceptable Use Agreement

This Acceptable Use Agreement is intended to ensure:

- that community users of academy digital technologies will be responsible users and stay safe while using these systems and devices
- that academy systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use academy systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the academy:

- I understand that my use of academy) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into academy for any activity that would be inappropriate in a academy setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the academy on any personal website, social networking site or through any other means, unless I have permission from the academy.
- I will not, without permission, 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 academy device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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).
- I understand that if I fail to comply with this Acceptable Use Agreement, the academy has the right to remove my access to academy systems / devices

I have read and understand the above and agree to use the academy digital technology 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: .....
Signed: .....
Date: .....

Appendix 7: Academy Policy Template: Electronic Devices-Searching & Deleting

Introduction
The changing face of information technologies and ever increasing student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to academy's by statute to search students in order to maintain discipline and ensure safety. Academies are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the academy will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the academy with justification for what it does.

The particular changes we deal with here are the added power to search for items 'banned under the academy rules' and the power to 'delete data' stored on seized electronic devices.
Items banned under the academy rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the academy rules may only be searched for under these new powers if it has been identified in the academy rules as an item that can be searched for. It is therefore important that there is a academy policy which sets out clearly and unambiguously the items which:

- are banned under the academy rules; and
- are banned AND can be searched for by authorised academy staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the academy rules.
Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
The Head Teacher / Principal must publicise the academy behaviour policy, in writing, to staff, parents / carers and students at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).
DfE advice on these sections of the Education Act 2011 can be found in the document:
"Screening, searching and confiscation – Advice for head teachers, staff and governing bodies" (2014 and updated January 2018)
http://www.education.gov.uk/academys/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

It is recommended that Principals (and, at the least, other senior leaders) should be familiar with this guidance.
Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The Academy Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012

- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

This is not a full list of Acts involved in the formation of this advice. Further information about relevant legislation can be found via the above link to the DfE advice document.

Responsibilities

The Principal is responsible for ensuring that the academy policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Principal will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: Safeguarding and Health and Safety Lead Officer / LGB Safeguarding governor/ ICT technician and ICT solutions

The Principal has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: Safeguarding leads and pastoral staff

The Principal may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Members of staff (other than Security Staff) cannot be required to carry out such searches. They can each choose whether or not they wish to be an authorised member of staff.

Training / Awareness

It is essential that all staff should be made aware of and should implement the academy's policy. Members of staff should be made aware of the academy's policy on "Electronic devices – searching and deletion":

- at induction
- at regular updating sessions on the academy's online safety policy

Members of staff authorised by the Principal to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

Policy Statements

Search:

The academy Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

The academy will already have a policy relating to whether or not mobile phones and other electronic devices are banned, or are allowed only within certain conditions. The academy should therefore consider including one of the following statements in the policy:

Students are allowed to bring mobile phones or other personal electronic devices to academy and use them only within the rules laid down by the academy. The Behaviour Policy lists the conditions under which they are allowed.

The sanctions for breaking these rules can be found in the Behaviour Policy.

Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the academy rules.

- Searching with consent - Authorised staff may search with the pupil's consent for any item
- Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the academy rules as an item which is banned and may be searched for

In carrying out the search:

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the academy rules and which can be searched for. (Whether there are 'reasonable grounds' is a matter decided on by reference to the circumstances witnessed by, or reported to, someone who is authorised and who exercises properly informed professional judgment and has received appropriate training).

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search. (The powers included in the Education Act do not extend to devices owned (or mislaid) by other parties e.g. a visiting parent or contractor, only to devices in the possession of students.)
The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the student being searched.
The authorised member of staff carrying out the search must be the same gender as the student being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student being searched.
There is a limited exception to this rule: Authorised staff can carry out a search of a student of the opposite gender including without a witness present, <u>but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.</u>

Extent of the search:
The person conducting the search may not require the student to remove any clothing other than outer clothing.

Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).

'Possessions' means any goods over which the student has or appears to have control – this includes desks, lockers and bags. (academys will need to take account of their normal policies regarding religious garments / headwear and may wish to refer to it in this policy)

A student's possessions can only be searched in the presence of the student and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the academy rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the academy rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the academy open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of academy discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

- child sexual abuse images (including images of one child held by another child)
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation. The academy should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff. The academy may wish to add further detail about these arrangements.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the

data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the academy rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of academy discipline) or whether the material is of such seriousness that it requires the involvement of the police.

A record should be kept of the reasons for the deletion of data / files. (DfE guidance states and other legal advice recommends that there is no legal reason to do this, best practice suggests that the academy can refer to relevant documentation created at the time of any search or data deletion in the event of a student, parental or other interested party complaint or legal challenge. Records will also help the academy to review online safety incidents, learn from what has happened and adapt and report on application of policies as necessary).

Care of Confiscated Devices
Academy staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices).
The academy may wish to add a disclaimer to the relevant section of the Behaviour Policy which may assist in covering the academy against damage / loss claims.

Audit / Monitoring / Reporting / Review
The responsible person Safeguarding Officer and Assistant Safeguarding Officer will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by the Designated Safeguarding Lead termly.
This policy will be reviewed by the head teacher and governors annually and in response to changes in guidance and evidence gained from the records.
The academy is required is publish its Behaviour Policy to parents annually (including on its website) – the Behaviour Policy should be cross referenced with this policy on search and deletion.
DfE guidance can be found at: https://www.gov.uk/government/publications/searching-screening-and-confiscation

APPENDIX 8: Social Media Policy Template

Scope
This policy is subject to the academy's Codes of Conduct and Online safety and Acceptable Use of ICT Agreements.
This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the academy.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education

The academy respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the academy's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a academy account or using the academy name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the academy or impacts on the academy, it must be made clear that the member of staff is not communicating on behalf of the 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 academy are outside the scope of this policy.

Digital communications with students are also considered. Staff may use social media to communicate with learners via a academy social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

SLT:

- Facilitating training and guidance on Social Media use.
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incidents.
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
- Receive completed applications for Social Media accounts
- Approve account creation

Administrator / Moderator:

- Create the account following SLT approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

Staff:

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via academy accounts
- Adding an appropriate disclaimer to personal accounts when naming the academy

Process for creating new accounts

The academy community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a "Friends of the academy" Facebook page. Anyone wishing to create such an account must present a business case to the Academy Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the academy has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the academy, including volunteers or parents.

Monitoring

Academy accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a academy social media account.

Behaviour

- The academy requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. Academy social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the academy.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to academy activity.
- If a journalist makes contact about posts made using social media staff must follow the academy media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the academy and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with academy policies. The academy permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

- The academy will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the academy will deal with the matter internally. Where conduct is considered illegal, the academy will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
- Handling abuse
- When acting on behalf of the academy, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, academy users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed academy protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

Academy use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the academy's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
- Under no circumstances should staff share or upload student pictures online other than via academy owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on academy social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any academy list of children whose images must not be published.
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use
Staff:

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

Students:

- Staff are not permitted to follow or engage with current or prior students of the academy on any personal social media network account.
- The academy's education programme should enable the students to be safe and responsible users of social media.
- Students are encouraged to comment or post appropriately about the academy. Any offensive or inappropriate comments will be resolved by the use of the academy's behaviour policy

Parents/Carers:

- If parents/carers have access to a academy learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The academy has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
- Parents/Carers are encouraged to comment or post appropriately about the academy. In the event of any offensive or inappropriate comments being made, the academy will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the academy's complaints procedures.

Monitoring posts about the academy

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

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the academy logo and/or branding on personal accounts

- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

Managing academy social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the academy
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the academy's reporting process
- Consider turning off tagging people in images where possible

The Don'ts

- Don't make comments, post content or link to materials that will bring the academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances

APPENDIX 9: Trust Password Policy
Version Control

Number	Description & Date	Author/Reviewer
0.1	**Final - July 2020**	**RH (RM)**

Introduction

Passwords help protect our data and systems. However, they are just part of what prevents hackers gaining access to systems. In designing this policy, we have reviewed **National Cyber Security Centre Password Guidance:**

https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

In particular, the paragraph:

Don't enforce regular password expiry

Regular password changing harms rather than improves security. Many systems will force users to change their password at regular intervals, typically every 30, 60 or 90 days. This imposes burdens on the user and there are costs associated with recovering accounts.

Forcing password expiry carries no real benefits because:

- *the user is likely to choose new passwords that are only minor variations of the old*
- *stolen passwords are generally exploited immediately*
- *resetting the password gives you no information about whether a compromise has occurred*
- *an attacker with access to the account will probably also receive the request to reset the password*
- *if compromised via insecure storage, the attacker will be able to find the new password in the same place*

Instead of forcing expiry, you should counter the illicit use of compromised passwords by:

- *ensuring an effective movers/leavers process is in place*
- *automatically locking out inactive accounts*
- *monitoring logins for suspicious behaviour (such as unusual login times, logins using new devices)*
- *encouraging users to report when something is suspicious*

You can also mitigate the risk of compromised accounts by using MFA, which will make a compromised password less useful to an attacker. Some MFA methods (such as SMS or email notifications) can even warn the user that they have been compromised, as they will receive a code when they did not request it. If you are using this form of MFA, you should encourage users to report this behaviour through your training.

Trust Core policy

With regards to the National Cyber Security Centre guidance, we use RM Unify (Single Sign on) and MFA (Multi Factor Authentication) to help protect access to Microsoft Office 365.

Please see Appendix 1 – RM Unify Password Policy below. This includes the RM Unify password complexity rules.

Appendix 1:

RM Unify Password Policy (updated Feb 2020) Please see link below for current version.

https://rmi.rmplc.net/Support/TechnicalArticle.asp?cref=TEC5943089

Foreword

When logging on to RM Unify, the user provides a password to verify their identity. It is important for the password to be hard for others to guess, but easy for the user to remember. Based on a recent analysis, looking at six million leaked passwords (obtained by hackers targeting various large Internet companies), over 99.8% occur in the top 10,000 common password list, with 91% in the top 1000 list. The main takeaway from this is that end users repeatedly choose passwords that are easy for a hacker to guess, in spite of today's password policies.

Heuristics, not composition rules

Composition rules are the traditional approach to ensure that a user sets a good quality password. For example: two lower case characters, one upper case, one symbol, and a maximum password length of 16 characters. Composition rules give a false sense of security, for example P@55word is a common, easy to guess password that is accepted by many traditional password policies. Following guidance of the UK and US government security agencies, RM Unify takes a different approach. Based on an open source research project from Dropbox.com, we use real world **heuristics** from hacker techniques to determine how strong a user's password is. RM Unify uses a password strength checker that, in seconds, can calculate a password's 'crackability'. This takes into account:

- Top 10,000 commonly used passwords
- Common dictionary words
- Common names in multiple languages
- 'L33t' substitution, e.g., 3 for e, 4 for a, $ for s, @ for a
- Keyboard spatial patterns, e.g., qwerty, 54321, zxcvbn

By deciding how 'crackable' a password is, RM Unify can ensure that your users' passwords meet a minimum threshold, making your passwords harder to guess.

Does this mean that passwords need to be long and hard to remember?

A hard to guess password does not mean that it needs to be hard to remember. It is true that longer passwords are generally harder to crack, but short passwords can also be strong. A passphrase would be ideal, but another approach is to choose two uncommon words and separate them with a space or symbol, for example, 'jade_walk' or 'clap cow' (we recommend you do not use these as actual passwords).

Scenarios for password changes

- **When a user changes their own password through RM Unify**
  The Change Password page gives instant feedback on the strength of the password and will not allow the password if it is weak (i.e. easily 'crackable'). This real-time feedback to the user on the quality of their password encourages less predictable passwords and aims to help educate users on good password hygiene.
- **Passwords synced to the cloud from RM Unify Network Agent or RM Unify AD Sync**
  When RM Unify receives a password change in the cloud via the RM Unify Network Agent, it is evaluated using our password policies. If the password is less than four characters long and does not meet the policies, this will be shown in the User Audit in Management Console and the user's password will not be updated in RM Unify. This will result in the local AD and RM Unify passwords being out of sync.

  RM Unify accepts passwords received from RM Unify AD Sync as long as the password meets the local network password policy.

  RM Unify has sophisticated safeguards to detect multiple attempts to guess a password and to prevent

unauthorised access. However, it is also good practice for schools to assess their own local network password policy when syncing accounts to any cloud service, not just when syncing to RM Unify.

- **User passwords set by an RM Unify privileged user**
  Where an RM Unify privileged user (RM Unify Super Admin, RM Unify Password Admin or RM Unify user with the Teaching Staff role) is changing an other user's password, the heuristics based rules are not applied. In these scenarios it is assumed that the privileged user is aware of the need for complex and secure passwords, and so feedback on the complexity requirements is of less concern, and the password will be changed at next logon. The only limitation is that the password chosen by the privileged must be at least four characters long and the 'User must change their password' box is ticked by default.

What control do I have as an RM Unify Super Admin?
At this point in time, RM have decided what the acceptable thresholds will be for each of the user types. We have set the bar for students slightly lower than other user types, as we understand that this class of user typically has less ability to remember long passwords and also has limited access to sensitive data.

In the future, RM plan to make the complexity thresholds configurable for each establishment. This would allow RM Unify Super Admins to set the bar differently for each user role. We recommend that you keep an eye on the RM Unify roadmap for when this functionality is released.

What if you really want to use composition rules?
We are sorry, but RM Unify cannot enforce composition rule based password policies. The UK Government and the entire tech industry alike have agreed that heuristic based policies, like those in action in RM Unify, are best practice.

More information
NIST is the US government's National Institute for Standards and Technology and is the world authority on authentication best practice. For more information on their recommendation to eschew composition rules, see section 5.1.1.2: https://pages.nist.gov/800-63-3/sp800-63b.html#memorized-secret-verifiers.

The UK's National Cyber Security Centre (NCSC) provides further information on why it now advises against forcing regular password expiry:
https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry

For more information on the approach we use, we recommend watching this presentation from Dan Wheeler (Dropbox): https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler.

To have a play with the Zxcvbn approach and see how it classifies different passwords, try the test site here:
https://lowe.github.io/tryzxcvbn/