THE CARLTON JUNIOR ACADEMY

REDHILL ACADEMY TRUST
Exsisto Optimus

Online Safety Policy

September 2019

Review: September 2020

We Grow Greatness

Online Safety Lead – Beth Hunter

Signed _____ Sharon Wood
Headteacher

Signed _____ Michelle Sills
Chair of Governors

Development/Monitoring/Review of this Policy

This Online Safety Policy has been developed by a working group made up of:

- Headteacher/Senior Leaders
- Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers

Consultation with the whole academy has taken place through a range of formal and informal meetings.

Schedule for Development/Monitoring/Review

This Online Safety Policy was approved by the Governing Body Committee on:	10th October 2019
The implementation of this Online Safety Policy will be monitored by the:	Headteacher: Sharon Wood Online Safety Governor: Lynne Thompson
The Governing Body will receive a report on the implementation of the Online Safety Policy (which will include anonymous details of online safety incidents) at regular intervals:	Annually: September
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. The next anticipated review date will be:	Annually: September
Should serious online safety incidents take place, the following persons/agencies should be informed:	Headteacher, Online Safety Lead, Chair of Governors, Safeguarding Lead, LADO or the Police

The academy will monitor the impact of the policy using:

- Logs of reported incidents
- Filtering by RM Broadband

Introduction and Overview

New technologies have become integral to the lives of children and young people in today's society, both within the academy and in their lives outside the academy. Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. The internet and other digital information 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 all to be more creative and productive in their work. Such technologies do present challenges and risks. We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way so they can reap the benefits of the online world.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the academy community at The Carlton Junior Academy with respect to the use of IT-based technologies.

- create a culture that incorporates the principles of online safety across all elements of academy life.
- safeguard and protect the children and staff of The Carlton Junior Academy.
- assist academy staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as Online Bullying.
- ensure that all members of the academy community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations being made against adults who work with pupils.

The main areas of risk for our academy community can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, extremism, radicalisation, ignoring age ratings in games (exposure to violence associated with often racist language) and substance abuse.
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites.
- Hate sites.
- Content validation: How to check authenticity and accuracy of online content.

Contact

- Grooming.
- Peer-on-Peer abuse.
- Cyber-bullying in all forms.
- Identity theft (including Facebook hijacking) and sharing passwords.

Conduct

- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent online or gaming).
- Sexting (sending and receiving of personally intimate digital/video images) also referred to as SGII (self-generated indecent images).
- Extremism/radicalisation.
- Copyright (little care or consideration for intellectual property and ownership – such as digital images and video, music and film).

Scope of the Policy

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

The Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. If the phone contains a pornographic image, headteachers have a statutory power to search or seize a pupils' phone.

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

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors who will receive regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor.

Online Safety Governor

The Online Safety Governor is responsible for ensuring they:

- attend regular safeguarding training.
- regularly meet with the Online Safety Lead.
- regularly monitor what is taught to children and staff.
- regularly monitor online safety incident logs.
- regularly monitor filtering.
- report to Governors.

Headteacher

The Headteacher is responsible for ensuring:

- she has a duty of care for the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- she is aware of the procedures that need to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents)
- that the Online Safety Lead receives suitable training to enable her to carry out her online safety roles and to train other colleagues, as relevant.
- that there is a system in place to allow for monitoring and support of those in academy who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- that the Senior Leadership Team and governors will receive regular monitoring updates from the Online Safety Lead.

Online Safety Lead

The Online Safety Lead is responsible for ensuring:

- that the academy delivers online safety content within the curriculum and embed it within the wider academy community.
- she takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the academy's Online Safety policy and other policies which include content relevant to teaching pupils how to use the internet safely.
- she keeps up-to-date with new challenges and risks.
- that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- she provides training and advice for staff.
- she liaises with academy technical staff.
- she receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

- she consults with stakeholders, including parents/carers and pupils about online safety provision so that the academy can capture information about experiences of emerging issues she is hearing about or facing online.
- she proactively engages staff, pupils, parents/carers and governors in academy activities that promote the agreed principle of online safety.
- she maps and reviews the online safety/digital literacy provision to give relevance, breadth and progression.
- She meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering.
- she reports regularly to Senior Leadership Team and governors.

Network Manager/Technical staff

The Technical Staff and Computing Lead are responsible for ensuring that:

- the academy's technical infrastructure is as secure as possible and is not open to misuse or malicious attack.
- the academy meets required online safety technical requirements.
- staff users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- any misuse of the network/internet/RMUnify/email is reported to the Headteacher or the Online Safety Lead.
- RM Broadband monitors internet activity.

Teaching and Support Staff

The teaching and support staff are responsible for ensuring:

- they have an up-to-date awareness of online safety matters and of the current academy Online Safety Policy and practices.
- they have read 'Keeping Children Safe in Education' and understand the advice for schools on embedding online safety into their broader safeguarding and child protection approach.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse or problem to the Headteacher/Senior Leader/Online Safety Lead for investigation/action/sanction.
- all digital communications with pupils/parents/carers should be on a professional level and are only carried out using official academy systems.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy and Acceptable Use Policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other academy activities (where allowed) and follow the academy's procedures with regard to these devices.
- they act as good role models in their use of digital technologies, the internet and mobile devices.
- in lessons where internet use is pre-planned, that they guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where pupils are allowed to freely search the internet, they should be vigilant in monitoring the content of the websites the young people visit.
- That from time-to-time, for good educational reasons, pupils may need to research topics (eg racism, drugs and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant

designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Designated Safeguarding Lead for Online Safety

The Designated Safeguarding Lead for Online Safety should be able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up-to-date capability required to keep children safe whilst they are online. Support will be given to teachers when they are delivering online safety content which may lead to a disclosure by a pupil. The Designated Safeguarding Lead for Online Safety will be involved when considering or planning online safety related lessons or activities as they will be best placed to reflect and advise on any known safeguarding cases and how to support any pupils who may be especially impacted by a lesson. They should be aware of the potential for serious child protection or safeguarding issues to arise from:

- sharing of personal data.
- access to illegal/inappropriate materials.
- inappropriate online contact with adults/strangers.
- potential or actual incidents of grooming.
- sexual exploitation (may occur without the child's immediate knowledge through copying digital videos or images that they have created and posted on social media).
- online-bullying.
- sexting/sexual harassment.
- abuse both sexual and emotional.
- Radicalisation.
- self-harm or harm to others.

Pupils

Pupils are responsible for:

- using the academy digital technology systems in accordance with the Pupil Acceptable Use Agreement.
- having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so.
- knowing and understanding policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- understanding the importance of adopting good online safety practice when using digital technologies out of the academy and realising that the academy's Online Safety Policy covers their actions out of the academy, if related to their membership of the academy.

Pupil Online Safety Leaders

Pupil Online Safety Leaders are responsible for:

- conducting assemblies to the whole academy about current online safety issues.
- offering peer-to-peer support about staying safe online.
- talking to parents about current online safety issues.
- writing online safety help tips on the academy newsletters.
- interviewing pupils to gain pupil voice about current online safety issues.
- helping to write the Pupil Acceptable Use Agreement.

Parents/Carers

Parents and 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 and information about national or local online safety campaigns. 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 digital/video images taken at school events.
- the parents' sections of the website and on-line programmes the academy uses.
- their children's personal devices in the academy (where this is allowed).
- social media.

Community Users

Community Users who access academy systems/website and other online programmes as part of the wider academy provision will be expected to sign a Community User AUA before being provided with access to academy systems.

Communication

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the academy website.
- Policy to be part of the academy induction pack for new staff.
- Acceptable Use Policy discussed with pupils at the start of each year.
- Acceptable Use Policy to be issued to whole academy community, usually on entry to the academy.
- Acceptable Use Policy for parents/carers and pupils are printed in the academy Personal Organiser.
- Acceptable Use Policies for all adults who are in the academy are held in the office.

Handling Complaints

- The academy will take all reasonable precautions to ensure that people are safe online. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an academy computer or mobile device.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

    1. Discussion with the Headteacher.
    2. Informing parents or carers.
    3. Removal of internet or computer access for a period.
    4. Referral to the Police.

- Any complaint about pupil misuse should initially be reported to the class teacher who then reports it to the Academy Business Leader, Headteacher or Online Safety Lead.
- Any complaint about staff misuse is referred to the Headteacher and/or the Chair of Governors.
- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy.
- Complaints related to child protection are dealt with in accordance with the academy's child protection procedures.

Education

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the academy's online safety provision. Children and young people need the help and support of the 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 embed 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:

- Providing Online Safety as part of the Computing Curriculum, PSHE Curriculum, SRE Curriculum, British Values and Citizenship Curriculum and the various curricula will complement each other to offer a fully rounded education.
- Embedding Online Safety across the curriculum and within the wider academy approach.
- Taking part in Internet Safety Day annually.
- Reinforcing key online safety messages in assemblies.

Pupils should:

- STOP and THINK before they CLICK.
- use YAPPY and ZIP IT, BLOCK IT, FLAG IT to stay safe online.
- Pupils should be taught that being online can put them at risk of sexual abuse, emotional abuse and peer-on-peer abuse.
- understand why and how some people will 'groom' young people for sexual or radicalisation reasons.
- 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. (The Counter Terrorism and Securities Act 2015 which requires academies to ensure that children are safe from terrorist and extremist material on the internet).
- understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- be aware that anyone can watch live streaming and can share live streams through other Apps if the privacy settings on each App is not switched on.
- understand how video/digital images can be manipulated and how web content can attract the wrong sort of attention.
- understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings.
- understand why they must not post pictures or videos of others without their permission.
- know not to download any files – such as music files - without permission.
- have strategies for dealing with receipt of inappropriate materials.
- know how to report any abuse including online bullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. Parent/Carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.
- be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information.
- be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- be aware that the author of a website/page may have a particular bias or purpose and to develop skills to recognise what that may be.
- know how to narrow down or refine a search understanding how search engines work and that this affects the results they see at the top of the listings.
- understand the issues around aspects of the commercial use of the internet, as age-appropriate. This may include risks in pop-ups, buying online and online gaming or gambling.
- be helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside of the academy.

Pupil Online Safety Leaders

Pupil Online Safety Leaders will spend time with the Online Safety Lead to gain understanding of current online safety issues so they can carry out their role to educate fellow pupils.

Vulnerable Pupils

Any pupil can be vulnerable online, and their vulnerability can fluctuate depending on their age, development stage and personal circumstance. However there are some pupils, for example looked after children and those with special educational needs, who may be more susceptible to online harm or have less support from family and friends in staying safe online. Therefore the curriculum will be tailored to ensure these pupils receive the information and support they need.

Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children 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, website.
- Parents'/Carers' evenings and sessions.
- High profile events/campaigns e.g. Safer Internet Day.
- Sending home the Digital Parenting Magazine and other information sheets.
- Reference to the relevant websites/publications on the academy website (see appendix for further links/resources).

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.
- Targeting Online Safety messages towards grandparents and other relatives as well as parents.
- Providing online safety information for the wider community via the academy website.

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.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the academy's Safeguarding procedures, Online Safety Policy and Acceptable Use Agreements.
- The Online Safety Lead 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 meetings.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Governors

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

- Attending training provided by the Local Authority/MAT/National Governors Association/or other relevant organisation if available.
- Participating in academy training/information sessions for staff or parents. This may include attending assemblies or lessons.

Technical – infrastructure/equipment, filtering and monitoring

The academy works with GBMicros who ensure that the academy is as secure as possible with the current systems that are in place.
In regards to the anti-virus the academy uses ESET. This will ensure that the anti-virus is then fully maintained and monitored.
The current systems ensure that:

- users can only access data to which they have right of access.
- no user can access another's files in their home area.
- access to personal data is securely controlled in line with the academy's Personal Data Policy.
- there is effective guidance and training for users.
- there is monitoring from senior leaders and these have impact on policy and practice.
- academy technical systems are managed in ways that ensure the academy meets recommended technical requirements.
- there will be regular reviews and audits of the safety and security of the academy's technical systems.
- servers, wireless systems and cabling are securely located and physical access restricted.
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.
- responsibilities for the management of technical security are clearly assigned to GBMicros.
- all users will have clearly defined access rights to academy technical systems.
- users will be made responsible for the security of their username and password and must not allow other users to access the systems using their log-in details and must immediately report any suspicion or evidence that there has been a breach of security.
- the domain/administrator passwords for the academy ICT systems, used by the Network Manager (or other person) must also be available to the academy on request.

- GBMicros are 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.
- academy technical staff regularly monitor and record the activity of users on the academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- remote management tools are used by staff to control workstations and view users activity.
- an appropriate system is in place for users to report any actual/potential technical incident to the Online Safety Lead or Technician.
- the academy has regular maintenance evenings where workstations are protected by up-to-date software to protect against malicious threats from viruses.
- internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by RM Broadband.
- internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- the academy has provided enhanced and differentiated user-level filtering.
- an agreed procedure is in place for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the academy systems.
- an agreed procedure is in place that forbids staff from downloading executable files and installing programmes on academy devices.
- an agreed procedure is in place regarding the use of removable media (eg memory sticks/ CDs/DVDs) by users on academy devices.

Sexting

In the latest advice for academies and colleges (UKCCIS, 2016), sexting is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'. 'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

What to do if an incident involving 'sexting' comes to your attention:

- Report it to your Designated Safeguarding Lead (DSL) immediately.
- Never view, download or share the imagery yourself, or ask a child to share or download – this is illegal.
- If you have already viewed the imagery by accident (e.g. if a young person has shown it to you before you could ask them not to), report this to the DSL.
- Do not delete the imagery or ask the young person to delete it.
- Do not ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- Do not share information about the incident to other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- Do not say or do anything to blame or shame any young people involved.
- Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL. Our academy's safeguarding policies outline codes of practice to be followed.

Passwords

The Carlton Junior Academy:

- ensures all staff have their own unique username and private passwords to access academy systems which are changed on a regular basis.

- makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.

Mobile Technologies (including BYOD/BYOT)

BYOD=Bring Your Own Device
BYOT=Bring Your Own Technology

Mobile technology devices may be academy owned/provided or personally owned 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 cloud based services such as email and data storage.
All users should understand that the primary purpose of the use mobile/personal devices in an academy context is educational. The mobile technologies usage is consistent with and inter-related to other relevant academy polices including the Safeguarding Policy, Behaviour Policy, Anti-bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the academy's Online Safety education programme.

The academy allows:

	Academy Devices			Personal Devices		
	Academy owned for single user	**Academy owned for multiple users**	**Authorised device[1]**	**Pupil owned**	**Staff owned**	**Visitor owned**
Allowed in academy	Yes	Yes	Yes	Yes with permission from SLT	Yes	Yes with permission from SLT
Network access	Yes	Yes	Yes	No	No	No
Internet only	No	No	No	No	Yes	Yes with permission from SLT
Cloud access	Yes	Yes	Yes	No	Yes	Yes with permission from SLT

Personal mobile phones and mobile devices

- Personal devices are brought into the academy entirely at the risk of the owner and the decision to bring the device in to the academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in academy.
- The academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at academy or on activities organised or undertaken by the academy.
- The academy accepts no responsibility for any malfunction of a device due to changes made to the device while on the academy network or whilst resolving any connectivity issues.

- Staff/Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements.
- Staff/Visitors bringing in mobile phones and mobile devices to the academy must not upload any content taken in academy to social media sites.
- All visitors are requested to keep their phones on silent.
- The academy reserves the right to search the content of any mobile phones and mobile devices on the academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.
- The bluetooth or similar function of mobile phones and mobile devices should not be used to send digital/video images or files to other mobile phones.
- Staff/Visitors can only access academy internet with permission from the SLT and should use in line with local safeguarding arrangements.
- Staff/Visitors should be mindful of the age limits for apps and software on their devices and should not use inappropriate age rated sites/apps in the academy.

Pupils' use of Personal Devices

- The academy strongly advises that pupil mobile phones and mobile devices should not be brought into the academy. If a mobile phone is discovered in a child's possession during the academy day, the parent/carer will be called to collect it from the academy office.
- If a pupil needs to bring in a mobile phone for usage after school, the mobile phone must be handed into the office at the beginning of the school day where it will be locked away until the end of the school day.
- If a pupil needs to contact parents/carers, they will be allowed to use an academy phone. Parents are advised, if they need to contact their child during the school day, to contact the academy office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of Personal Devices

- No digital/video images should be taken in the academy on staff handheld devices, including mobile phones, iPads and personal cameras.
- Staff must leave their mobile phone in the staffroom whilst children are in the academy and may only have them on their person if permission has been given by the Headteacher.
- Where staff members are required to use a mobile phone for academy duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances.
- Printing from personal devices will not be possible.
- If a member of staff breaches the academy policy, then disciplinary action may be taken.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of digital/video images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital/video images on the internet. Such digital/video images may provide avenues for online bullying to take place. Digital/Video 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.

- Written permission from parents or carers will be obtained before any digital/video images of pupils are published on the academy website, Class Dojo, social media, academy promotional materials and in the local press. These digital/video images can still be used once the pupil has left the academy or for a limited time.
- When using digital/video images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of digital/video images. In particular they should recognise the risks attached to publishing their own digital/video images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents/ carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases child protection, these digital/video images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- 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 digital/video images. Those digital/video images should only be taken on academy equipment, the personal equipment of staff should not be used for such purposes.
- As part of their work, pupils will have access to the use of digital cameras/iPads. Any digital/video images that they take, will be kept at the academy and the children will be taught about the need to keep these digital/video images private. When on academy visits, pupils are not allowed to take their own cameras or use cameras on phones without permission.
- Location Tags must not be used when taking digital/video images.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute digital/video images of others without their permission.
- Digital/Video images published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such digital/video images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with digital/video images
- LAC pupils will never have digital/video images used online unless the academy has permission from the carers to do so.
- The academy will periodically invite an official photographer into school to take portraits/photographs of individual children and/or class groups. The academy will undertake its own risk assessment in terms of the validity of the photographer/agency involved and establish what checks/vetting has been undertaken.
- Digital/Video images are stored on a secure area on the server or on RMUnify and should not be stored on portable external hard drive devices.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, academies are likely to be subject to greater scrutiny in their care and use of personal data.
Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.
The academy has ensured that it has a GDPR Policy, Pupil and Staff Privacy Notices and a Trust Data Acceptable use Statement.

Communications

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

- The official academy email service may be regarded as safe and secure and is monitored.
- Users should be aware that email communications can be monitored.
- Users must immediately report, to the nominated persons – 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.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, etc.) must be professional in tone and content. These communications may only take place on official academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils may be provided with individual academy email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Users should know that spam, phishing and virus attachments can make emails dangerous.
- Users should know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on academy headed paper.
- Users should know that the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
- Personal information should not be posted on the academy website.
- The academy does not publish personal email addresses of pupils or staff on the academy website. There is a link to staff email so that children can hand in homework but the staff email address cannot be seen by users of the website.

Social Media - Protecting Professional Identity

Our academy has a duty of care to provide a safe learning environment for pupils and staff. The academy could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy liable to the injured party. Reasonable steps to prevent predictable harm must be in place.
The academy provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the academy through:

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

Academy staff should ensure that:

- no reference should be made in social media to pupils, parents/carers or academy staff.
- they do not engage in online discussion on personal matters relating to members of the academy community.
- personal opinions should not be attributed to the academy.
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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

- a process for approval by senior leaders.
- a clear processes for the administration and monitoring of these accounts – involving at least two members of staff.
- a code of behaviour for users of the accounts.
- systems for reporting and dealing with abuse and misuse.
- an understanding of how incidents may be dealt with under academy disciplinary procedures.

Personal Use

- Personal communications are those made via 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.
- The academy permits reasonable and appropriate access to private social media sites.
- Where excessive personal use of social media in the academy is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

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.
- 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 Senior Leadership Team to ensure compliance with the academy policies.

Academy Website/App

- The Headteacher takes overall responsibility to ensure that the website/app content is accurate and the quality of presentation is maintained.
- The academy website complies with the statutory DfE guidelines for publications.
- Most material is the academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the website/app is the academy address, telephone number and we use a general email contact address. Home information or individual email identities will not be published.
- Digital/Video images published on the website do not have full names attached.
- We do not use pupils' names when saving digital/video images in the file names or in the tags when publishing to the academy website/app.
- We expect teachers using academy approved blogs or wikis to password protect them and run from the academy website/app.

Cloud-Based Technologies

- Uploading of information on the academy's RMUnify is shared between different staff members according to their responsibilities.
- Digital/Video images uploaded to the academys systems will only be accessible by members of the academy community.

Live Streaming

- Ensure if you are streaming in academy that it doesn't congest the internet causing it to run more slowly for others.
- All pupils are supervised by a member of staff when streaming.
- All members of staff have a good knowledge of what they are streaming before they start.
- Facebook Live, Instagram Live and YouTube Live are not used to live stream in the academy. Skype may be used but permission needs to be sought from the Computing Leader. Participants in live streams offered may not be DBS checked so a member of staff must always be present.
- Misuse of streaming by any member of the academy community will result in sanctions.

Video Conferencing

- We only use the approved services for video conferencing activity.
- Permission is sought from parents/carers if their children are involved in video conferencing.
- All pupils are supervised by a member of staff when video conferencing.
- Approval from the Headteacher/SLT is sought prior to all video conferences within the academy.
- The academy conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

Webcams

- We do not use publicly accessible webcams in the academy.
- Webcams in the academy are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the academy community will result in sanctions.

Games Machines

Games machines including Sony PlayStation, Nintendo Wii, Microsoft Xbox and others which have Internet Access are only allowed to be used in officially sanctioned locations and under supervision.

- Pupils will discuss safe and appropriate use of online gaming sites. They will be given gaming dilemmas and discuss the scenarios.
- Pupils will not play online games against unknown players at the academy.
- Pupils will understand the risks of online gaming especially websites that involve chatrooms.
- Pupil will be aware that they can become addicted to the 'virtual world.'

Dealing with unsuitable / inappropriate activities

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

User Actions		Acceptable at certain times	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
	Maliciously corrupt or erase data or programs. Contrary to the Computer Misuse Act 1990.			X
	Promotion of any kind of discrimination. Contrary to the Racial and Religious Hatred Act 2006 and the Public Order Act 1986.			X
	Threatening behaviour, including promotion of physical violence or mental harm. Contrary to the Malicious Communications Act 1988.			X
	Promotion of extremism or terrorism. Contrary to the Racial and Religious Hatred Act 2006.			X

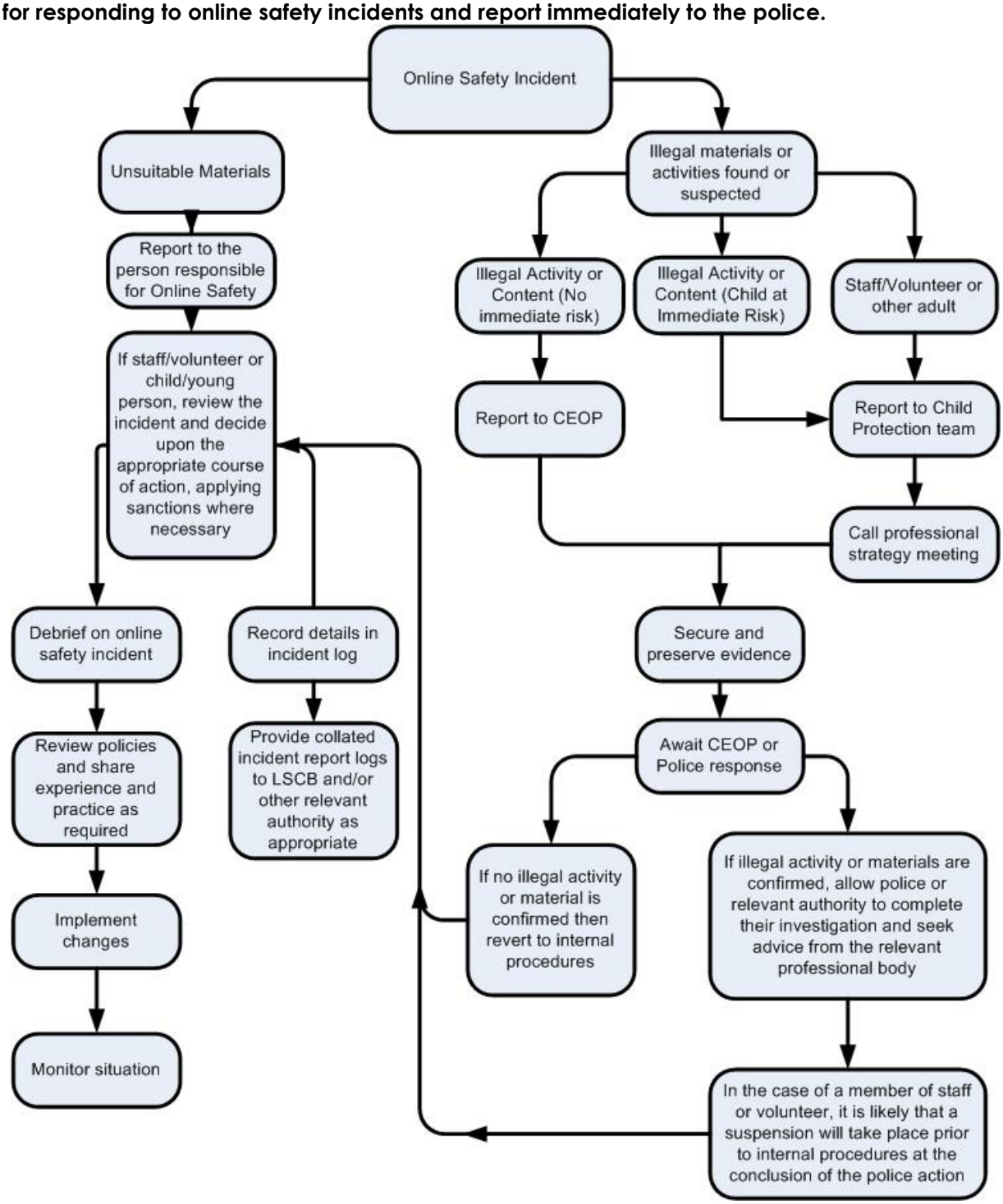
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute. .Contrary to the Communications Act 2003.			X
	Using academy systems to run a private business. Contrary to the Computer Misuse Act 1990. .			X
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the academy. Contrary to the Regualtion of Investigatory Powers Act 2000.			X
	Infringing copyright. Contrary to the Copyright, Design and Patents Act 1988.			X
	Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/network access codes and passwords). Contrary to the Computer Misuse Act 1990.			X
	Creating or propagating computer viruses or other harmful files. Contrary to the Computer Misuse Act 1990.			X
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	
On-line gaming (educational)		X		
On-line gaming (non-educational)			X	
On-line gambling			X	
On-line shopping / commerce		X		
File sharing		X		
Use of social media		X		
Use of messaging apps		X		
Use of video broadcasting e.g. YouTube		X		

Responding to incidents of misuse

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

Illegal Incidents

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



Other Incidents

It is hoped that all members of the academy community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse

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

- Have more than one senior member of staff 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 of Redhill Academy Trust 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.

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Academy Actions & Sanctions

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Pupil Incidents	Refer to Headteacher/Online Safety Lead	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	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	X	X	X
Unauthorised use of non-educational sites during lessons	X		X	X	X	X
Unauthorised/inappropriate use of mobile phone / digital camera/other mobile device	X		X	X	X	X
Unauthorised/inappropriate use of social media / messaging apps/personal email	X		X	X	X	X
Unauthorised downloading or uploading of files	X		X	X	X	X
Allowing others to access academy network by sharing username and passwords	X		X	X	X	X
Attempting to access or accessing the academy network, using another student's pupil's account	X		X	X	X	X
Attempting to access or accessing the academy network, using the account of a member of staff	X		X	X	X	X
Corrupting or destroying the data of other users	X		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	X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X	X	X	X
Using proxy sites or other means to subvert the academy's filtering system	X		X	X	X	X
Accidentally accessing offensive or pornographic material	X		X	X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes GDPR	X		X	X	X	X

Staff Incidents	Refer to Headteacher/Online Safety Lead	Refer to Local Authority	Refer to Police	Refer to Technical Support	Warning	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)	X	X	X	X		X
Inappropriate personal use of the internet/social media/personal email	X	X	X	X	X	X
Unauthorised downloading or uploading of files	X			X	X	X
Allowing others to access academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	X			X	X	X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X		X	X	X
Deliberate actions to breach data protection or network security rules	X			X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X		X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing	X	X	X	X	X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	X	X	X	X	X	X
Using proxy sites or other means to subvert the academy's filtering system	X		X	X	X	X
Accidentally accessing offensive or pornographic material	X			X		
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X
Breaching copyright or licensing regulations	X		X	X	X	X

Asset Disposal

All redundant equipment will be disposed of through an authorised agency. All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The academy will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Appendices

Posters to be displayed in academy

ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.

FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

The Carlton Junior Academy (Staff (and Volunteer) Acceptable Use Policy Agreement

Academy Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. 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 pupils 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 pupils 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, RMUnify etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- 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 not save my personal academy data, the personal data of others or digital/video images of pupils on a removable hard drive/USB device unless it is encrypted.
- I will not save my personal academy data, the personal data of others or digital/video images of pupils on a personal device.
- I will only use RMUnify as a cloud based technology to save my personal academy data, the personal data of others or digital/video images of pupils.
- I understand that digital and video images taken of me can be displayed in the academy and in the Redhill Trust publications and used on the academy and Redhill Trust website/app.

I will be professional in my communications and actions when using academy IT 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 digital/video 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 digital/video images. Where these digital/video images are published 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 the academy in accordance with the academy's policies.
- I will only communicate with pupils and parents/carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will be aware that my relationships and association online may have safeguarding implications and I should avoid online contact with individuals that have been disqualified from working with children.

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

- When I use my mobile devices (laptops/tablets/mobile phones/USB devices etc) in the 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 Academy GDPR 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 pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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 the 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 Governors, Headteacher 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 the academy) and my own devices (in the academy and when carrying out communications related to the academy) within these guidelines.

Staff/Volunteer Name: .....
Role in academy: .....
Signed: .....
Date: .....

The Carlton Junior Academy Acceptable Use Agreement for Community Users

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 the academy for any activity that would be inappropriate in an 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 digital/video images of others I will only do so with their permission. I will not use my personal equipment to record these digital/video images, without permission. If digital/video 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 an 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 the academy) and my own devices (in the academy and when carrying out communications related to the academy) within these guidelines.

Name: ..... Signed: .....

Date: .....

Record of Reviewing Devices

Person using device:.....
Date: .....
Reason for investigation:.....
.....
.....

Details of first reviewing person
Name: .....
Position: .....
Signature: .....

Details of second reviewing person
Name: .....
Position: .....
Signature: .....

Device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log Group:						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log Group:				
Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Legislation

At the Carlton Junior Academy, we are aware of the legislative framework under which this Online Safety Policy and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.
It is recommended that legal advice is sought in the advent of an online safety issue or situation.

Computer Misuse Act 1990
This Act makes it an offence to

- erase or amend data or programs without authority.
- obtain unauthorised access to a computer.
- "eavesdrop" on a computer.
- make unauthorised use of computer time or facilities.
- maliciously corrupt or erase data or programs.
- deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be

- fairly and lawfully processed.
- processed for limited purposes.
- adequate, relevant and not excessive.
- accurate.
- not kept longer than necessary.
- processed in accordance with the data subject's rights.
- secure.
- not transferred to other countries without adequate protection.

General Data Protection Regulation (GDPR) May 25, 2018

The GDPR has applied to organisations across the world since 25 May 2018. With the UK now set to leave the European Union, the UK has formalised GDPR into new legislation under the Data Protection Act 2018. GDPR will now sit alongside DPA, however, in most cases, the DPA will be referred to as a matter of law. GDPR was designed to modernise laws that protect the personal information of individuals.

Before GDPR started to be enforced, the previous data protection rules across Europe were first created during the 1990s and had struggled to keep pace with rapid technological changes. GDPR alters how businesses and public sector organisations can handle the information of their customers. It also boosts the rights of individuals and gives them more control over their information.

Freedom of Information Act 2000
The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

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

- establish the facts.
- ascertain compliance with regulatory or self-regulatory practices or procedures.
- demonstrate standards, which are or ought to be achieved by persons using the system.
- investigate or detect unauthorised use of the communications system.
- prevent or detect crime or in the interests of national security.
- ensure the effective operation of the system.

Monitoring but not recording is also permissible, in order to

- ascertain whether the communication is business or personal.
- protect or support help line staff.

The academy reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

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

Copyright, Designs and Patents Act 1988

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

Telecommunications Act 1984

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

Criminal Justice & Public Order Act 1994

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

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

Racial and Religious Hatred Act 2006

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

Protection from Harassment Act 1997

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

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent digital/video images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a

digital/video image. A digital/video image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003
A grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998
This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the academy context, human rights to be aware of include

- the right to a fair trial.
- the right to respect for private and family life, home and correspondence.
- freedom of thought, conscience and religion.
- freedom of expression.
- freedom of assembly.
- prohibition of discrimination.
- the right to education.

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

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

The Education and Inspections Act 2011
Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012
Requires schools to seek permission from a parent/carer to use Biometric systems.

The School Information Regulations 2012
Requires schools to publish certain information on its website:
https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

Serious Crime Act 2015
Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE).

Keeping Children Safe in Education **2019**

This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014, and the Non-Maintained Special Schools (England) Regulations 2015. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children. For the purposes of this guidance children includes everyone under the age of 18.

Links to other Organisations or Documents

UK Safer Internet Centre
Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Internet Watch Foundation - https://www.iwf.org.uk/
LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE / Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/
CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Tools for Schools
Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self review tool: www.360data.org.uk

Bullying/Online-bullying/Sexting/Sexual Harassment
Enable – European Anti Bullying programme and resources (UK coordination / participation through SWGfL & Diana Awards) - http://enable.eun.org/
Scottish Anti-Bullying Service, Respect me - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Online bullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Online_bullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Online bullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/online bullying -guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/online bullying 1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking
Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children's Commissioner, TES and Schillings – Young peoples' rights on social media

Curriculum
SWGfL Digital Literacy & Citizenship curriculum
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Mobile Devices/BYOD
Cloudlearn Report Effective practice for schools moving to end locking and blocking
NEN - Guidance Note - BYOD

Data Protection
360data - free questionnaire and data protection self review tool

ICO Guide for Organisations (general information about Data Protection)

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

ICO Guidance on Bring Your Own Device

ICO Guidance on Cloud Computing

ICO - Guidance we gave to schools - September 2012

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support
UKSIC – Appropriate Filtering and Monitoring
Somerset - Questions for Technical Support
NEN – Advice and Guidance Notes

Working with Parents and Carers
SWGfL Digital Literacy & Citizenship curriculum
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops / education
The Digital Universe of Your Children - animated videos for parents (Insafe)
Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide
Insafe - A guide for parents - education and the new media

Research
EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011
Futurelab - "Digital participation - its not chalk and talk any more!"
Ofcom –Media Literacy Research

Glossary of Terms

AUP/AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.