Corsham Regis
Primary Academy

POLICY – ONLINE SAFETY

Date approved: January 2022
Date for next review: January 2023

Online Safety Policy

Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using computing. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources, e-mail and mobile learning, such as i.pads and tablets. Computer skills are vital to access life-long learning and employment; indeed, computing is now seen as an essential life-skill.

In line with academy policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks. The education of pupils 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 school to recognise and avoid Online Safety risks and build their resilience.

The policy includes policy and guidance on:

- Technical infrastructure
- Password and Filtering
- Acceptable Use Agreements
- Mobile Technologies
- Social Media
- Data Protection
- Use of digital and video images
- What to do in the event of an Online Safety Incident
- Online Safety Curriculum

This Online Safety policy has been developed by:

- Headteacher/Senior Leaders
- Staff
- Corsham Regis Governing Body (CRLGB)
- Parents and Carers

- Pupils

1. Why is internet use important?

- The purpose of internet use in the academy is to raise educational standards; to promote pupil achievement and well-being; to support the professional work of staff and to enhance both the academy's management information and administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The internet is an essential element in 21st century life for education, business and social interaction. The academy has a duty to provide students with quality internet access as part of their learning experience.

2. How will internet use enhance learning?

- The academy internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
- Pupils will learn appropriate internet use and be given clear objectives for internet use.
- Staff will guide pupils in online activities to support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

3. How will internet access be authorised?

- The academy will keep a record of all staff and pupils who are granted internet access, i.e. through the Acceptable Use Agreement for pupils and staff (**see Appendices 3 – 5**). The record will be kept up-to-date; for instance, a member of staff may leave or a pupil's access be withdrawn.
- Primary pupils' home-academy agreement will include a copy of the Acceptable Use Agreement for pupils and the Parent / Carer ICT Acceptable Use Agreement.
- Primary pupils will not be issued individual email accounts but will be authorised to use a class email address under supervision.
- Parents / Carers will be informed that pupils will be provided with supervised internet access.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering
- Internal monitoring data for network activity
- Communication with:
    - pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of the Corsham Regis community (including staff, pupils, governors, volunteers, parents / carers, visitors) who have access to and are users of the academy ICT 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 cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the academy, but is linked to membership of the academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

Corsham Regis 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 school.

Roles and Responsibilities

All staff including teachers, teaching assistants and support staff, and volunteers will be asked to sign the staff Acceptable Use Agreements and The Corsham School (ICT) Acceptable Use Policy (Part of The Corsham School Multi Academy Group's Personnel Policy)

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 receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Leader (the Headteacher)
- attendance at Academy Council meetings which have an online focus
- regular monitoring of online safety incident logs
- regular monitoring of filtering / change control logs
- reporting to the CRLGB

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher, who is also the Designated Safeguarding Lead, and the other Deputy Designated Safeguarding Leads, Mrs Sarah Harris and Mrs Gemma Morris, should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority and MAT disciplinary procedures).
- The Headteacher is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their online safety roles.

Admin and Finance Manager:

The Admin and Finance Manager 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 - academy group Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy 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 internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction

Teaching and Support Staff

Teachers 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 Agreement (AUA)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction

- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school 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 agreements
- 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 school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Academy Council

The Academy Council is a consultative group that has wide representation from pupils within the academy. One of its responsibilities is for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

Terms of reference for the Academy Council can be found later in this document as **Appendix 1**

Members of the Academy Council will assist the Headteacher with:

- the production / review / monitoring of the school Online Safety Policy / documents.
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision

Pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil 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 school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

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 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 school events.

Policy Statements

Education – Pupils

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

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

- A planned online safety curriculum (**see Appendix 2**) 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
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside the 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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

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, academy social media pages
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day

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:

- 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 Headteacher 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 Headteacher 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 responsible for safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).

- Participation in academy training / information sessions for staff or parents

Mobile Technologies (including Bring Your Own Devices/Technology)

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

All users should understand that the primary purpose of the use of mobile / personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

- The Corsham Regis Acceptable Use Agreements for staff, pupils, parents/carers, governors and volunteers will give consideration to the use of mobile technologies
- Corsham Regis allows:

	Academy Devices		Personal Devices		
	Academy owned for single user	**Academy owned for multiple users**		**Single user**	**Multiple users**
Allowed in school	*Yes*	*Yes*	Allowed in school	*Yes*	*No*
Full network access	*Yes*	*Yes*	Full network access	*No*	*No*
Internet only	*Yes*	*Yes*	Internet only	*No* *Guest logins for visiting professionals if required*	

- Corsham Regis has provided technical solutions for the safe use of mobile technology for school devices/personal devices:
    - Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
    - The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
    - For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
    - All school devices are subject to routine monitoring

- When personal devices are permitted:
    - Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school 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 school
    - Corsham Regis accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
    - Corsham Regis accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
    - Pupils in Year 6, who have permission to walk to and from school on their own, are permitted to bring in a mobile phone so that they can communicate with their family members in the event of an emergency when on their own as long as they have written permission from their parents/carers. The phone must be switched off and handed in to the class teacher when the child arrives in school and collected by the child at home time.
    - Pupils in all year groups may choose to have a Tech Party as a class reward. The school will provide iPads and computers to support this. However, some pupils may want to bring in their own mobile phone or personal device. They are permitted to do so if they wish. At the start of the day, for their own safety and that of others, access to 3G, 4G or 5G roaming data will be switched off and checked by the class teacher
    - Strong Pass-codes or PINs should be set on personal devices to aid security
    - Any mobile phone or personal device brought into school without permission will be confiscated and must be collected by the parent.
    - Whenever a pupil brings a phone, or mobile device, into school with permission, they will not have access to the school IT network.
    - Pupils are reminded that they are not allowed to take photographs of other pupils or staff with a personal mobile device.

- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements. In addition:
    - Devices may not be used in tests
    - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements

- Users are responsible for keeping their device up to date through software, security and app updates. The device must be virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school
- Personal devices should be charged before being brought to school as the charging of personal devices is not permitted during the school day
- Devices must be in silent mode on the school site
- School devices are provided to support learning.
- Confiscation and searching (In England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
- Corsham Regis will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
- Devices may be used in lessons in accordance with teacher direction
- Any personal device that has obvious Health and Safety defects should not be brought into school.
- The user is responsible for securing their device to prevent sensitive data from being lost or compromised and to prevent viruses from being spread. Removal of academy installed security controls is prohibited.
- Users are forbidden from copying sensitive data from email, calendar and contact applications to other applications on the device or to an unregistered personally owned device.
- School is not responsible for any financial cost charged to your account unless incurred during approved school-related use

Cyber Security Incidents

- If you believe you have received a malicious spam or phishing email, do NOT open it, or any attachment or follow any links within the email. Report the email immediately to the Headteacher who will advise on further steps to be taken*.
- If you receive an Anti-Virus pop up alert on your device, this may mean you have followed a malicious link, or visited a compromised website in error. Follow the steps as advised by the Anti-Virus programme, which is most cases will fix the problem. Report this to the Head immediately*.
- If you believe that your device has been infected with malware, disconnect it from any network cable or WiFi network immediately. On a laptop the fastest way to do this may be to put the device into airplane mode. Do NOT turn the device off as this can remove any evidence. Contact the Head immediately*

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 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 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. Corsham Regis 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press or used in promotional publications
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be 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 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 pupils are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection - following implementation of General Data Protection Regulations from 25th May 2018

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

For further information, please see the General Data Protection Regulation policy and Fair Process Privacy Notice for TCSAG.

Communications

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

	• Staff & other adults	• Pupils

Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the academy	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time	x							x
Taking photos on academy owned 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. Pupils should therefore use only the academy email service to communicate with others when in school
- 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.
- Any email communication between staff and pupils or parents / carers must be professional in tone and content.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

Corsham Regis recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the academy, its staff, parents, carers and children.

This document:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- 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

Corsham Regis respects privacy and understands that staff and pupils 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 group's reputation are within the scope of this policy.

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

Corsham Regis has a duty of care to provide a safe learning environment for pupils and staff, and 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 Corsham Regis or the academy group 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 school through:

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

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 school community
- Personal opinions should not be attributed to the academy or local authority
- 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
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- Organisational control of Social Media

Roles & Responsibilities

- **Senior Leadership Team (SLT)**
    - Facilitating training and guidance on Social Media use.
    - 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.
    - Approve account creation

- **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
    - Adding an appropriate disclaimer to personal accounts when naming the school

Process for creating new accounts

The Corsham Regis community is encouraged to consider if a social media account will help them in their work, e.g, a "Friends of the school" Facebook page. Anyone wishing to create such an account must present a business case to the Senior 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 school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

Monitoring

School social media 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 school social media account.

Behaviour

- The school 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 school.
- 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 school 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 school 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 school'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 pupil pictures online other than via Corsham Regis owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Pupils should be appropriately dressed, not be subject to ridicule and must not be on any school 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 school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
    - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Corsham Regis permits reasonable and appropriate access to private social media sites.

- **Pupil**
  - Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account.
  - Corsham Regis's education programme teaches pupils to be safe and responsible users of social media.
  - Any offensive or inappropriate comments will be resolved by the use of the academy's behaviour policy.

- **Parents/Carers**
  - Parents/Carers are encouraged to comment or post appropriately about Corsham Regis. 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, parents may be referred to The Corsham School Academy Group complaints procedures.

Guidance for all academy group staff using social media:

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 school 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 school social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the school
- 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 school'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 group 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 school 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

Unsuitable / inappropriate activities

How do we respond?

The Wiltshire Safeguarding Children Board flow charts entitled 'Allegations against adults – Risk of harm to children' and 'What to do if you are worried a child is being abused or neglected' must be referred to when managing an incident of concern about Internet use by a child, young person or member of staff or volunteer. Additional guidance can be found in the flow chart below (Fig 1)

General guidance following an incident

1) Record incidents on an Online Safety incident log sheet (see below) and keep this in the Child Protection file.

2) Ensure all appropriate staff are informed e.g. Senior Leadership Team, Designated Safeguarding Lead, Computing Subject Leader and the Chair of Governors.

3) After any investigations are completed it is essential to debrief, identify lessons learnt and implement any changes required.

4) If at any time you are unsure how to proceed, then contact the Wiltshire MASH

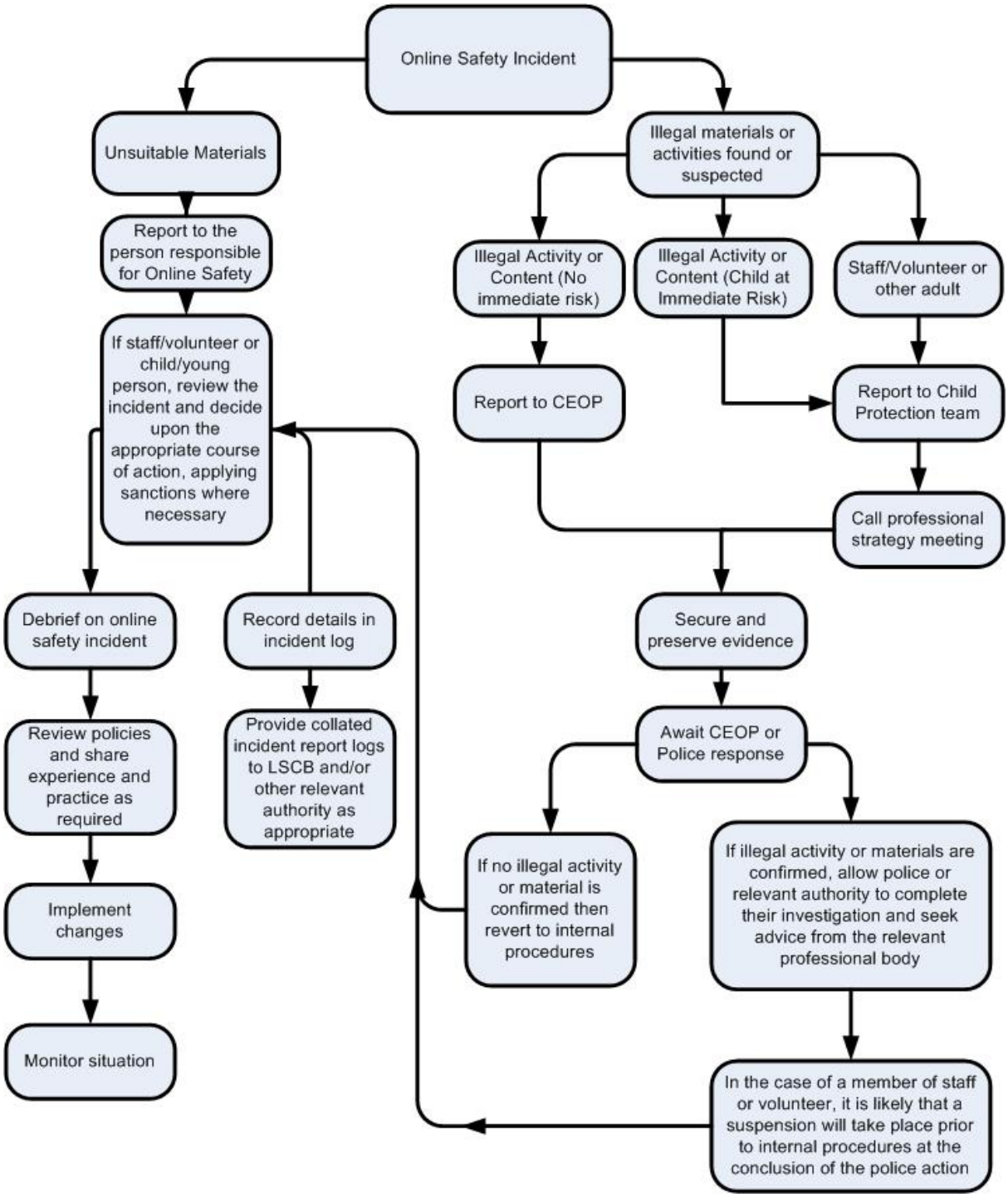
Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of

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.

Corsham Regis 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	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	

Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing				X	
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube		X			



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 (see above) 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 / 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 Local Authority / Academy Group 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 school 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:

	Actions / Sanctions								
Pupil Incidents	Refer to class teacher	Refer to Deputy Headteacher	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction 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								
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	X	
Attempting to access or accessing the academy network, using the account of a member of staff	X	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as	X	X	X			X	X	X	

offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X		X	X	X	X
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	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				
Inappropriate personal use of the internet / social media / personal email		X				X		X
Unauthorised downloading or uploading of files	X	X	X			X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X			X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X			X	X	X

Deliberate actions to breach data protection or network security rules	X	X	X	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	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	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	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X		X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X	X		X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Responding to an Incident: Police procedures

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the academy should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible, after contacting the Wiltshire MASH, if the offence is deemed to be out of the remit of the academy to deal with.

Where it is determined that an offence has been committed and that a police investigation is warranted, all measures to preserve evidence should be undertaken.

If an Officer decides that equipment needs to be seized, then they will need to determine if the equipment is networked. If in doubt as to whether the server should be seized or not, officers should seek advice from the Police Digital Forensic Unit, as seizure of the server will have a significant impact on the academy.

In cases where a suspect picture or photograph is discovered, including Sexting (**see Appendix 7**), it should also be borne in mind that a person could be guilty of the offence to 'Make' and 'Distribute' if they print or forward the image. There is a defence in law for these circumstances — in some cases, it may still be necessary for that person, or others (for example a person to whom an accidental find is

reported), to knowingly "make" another copy of the photograph or pseudo-photograph in order that it will be reported to the authorities, and clearly it is desirable that they should be able to do so without fear of prosecution. Digital or printed copies of indecent images of children will be seized.

In all cases a detailed statement may be obtained to assist those who investigate the offence. The following information may be included in the statement:

_ The identity of any material witnesses;
_ The name of the Internet service provider (ISP) or mobile telephone service provider in the case of images received through a telephone;
_ If known, the web address, name of the chat room or online group through which the image was found or received;
_ Any passwords or other procedure required to gain access to the website;
_ If known, the identity of the person who sent the image;
_ In the case of email, the sender's email address or the screen name used by the sender while in a chat room;
_ The reason for any delay in reporting the incident to the police (to assist investigators).

In the case of offences involving mobile technology where an incident arises which is deemed to be of a serious nature and necessitates criminal investigation, it may require the seizure of the telephone

Technical – infrastructure / equipment, password security, filtering and monitoring

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. Corsham Regis employs an outside contractor, MARCCs, to manage our IT system and network. Corsham Regis, with IT support from MARCCS, will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the TCSAG General Data Protection Regulation policy
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.
- there is an online system for staff to report any actual / potential technical incident to the IT support technician from MARCS
- the school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Servers, wireless systems and cabling are securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.
- 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.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.

Responsibilities

The management of technical security will be the responsibility of Admin and Finance Manager, Mrs Tracie Brewer

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices, email and Virtual Learning Environment (VLE).

- All users will have clearly defined access rights to academy technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Headteacher
- All academy networks and systems will be protected by secure passwords that are regularly changed
- The "administrator" passwords for the academy systems, used by the technical staff must also be available to the Headteacher or the Admin and Finance Manager, Mrs Tracie Brewer, and kept in a secure place
- All users (adults and pupils) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security to the Headteacher.
- Passwords for new users, and replacement passwords for existing users will be allocated by the Admin and Finance manager, Mrs Tracie Brewer

Pupil Passwords

- All users will be provided with a username and password by the class teacher to access their class folder and contents.
- All pupils in KS2 will be given a Mathletics username and password by the Mathematics Leader who will keep an up to date record of users and their usernames.
- Pupils will be taught the importance of password security

Training / Awareness

Members of staff will be made aware of the academy's password policy:

- at induction
- through the school's online safety policy
- through the Acceptable Use Agreement

Pupils will be made aware of the academy's password policy:

- in lessons when username and passwords are shared
- through the Acceptable Use Agreement

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger

strategy for online safety and acceptable use. It is important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in Corsham Regis.

Responsibilities

The responsibility for the management of the academy's filtering policy will be held by the Admin and Finance Manager, Mrs Tracie Brewer.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- be logged in change control logs
- be reported to a second responsible person, the Headteacher:

All users have a responsibility to report immediately to the Admin and Finance Manager or the Headteacher any infringements of the academy's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the academy. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the Corsham Regis network, filtering will be applied that is consistent with school practice.

Corsham Regis has provided differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils / SLT.)

Mobile devices that access the academy internet connection (whether academy or personal devices) will be subject to the same filtering standards as other devices on the school systems

Any filtering issues should be reported immediately to the filtering provider.

Requests from staff for sites to be removed from the filtered list will be considered by the Headteacher. These will only be approved if they provide an educational benefit to pupils.

Education / Training / Awareness

Pupils will be made aware of the importance of filtering systems through the online safety education. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

- the Acceptable Use Agreement
- induction training
- staff meetings, briefings, INSET.

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through online safety awareness sessions / newsletter etc.

Changes to the Filtering System

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the Headteacher who will decide whether to make school level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement.

Our internet is provided through Schoolcare while Lightspeed provide our filtering solution. This link shows the service which they offer.

http://www.saferinternet.org.uk/sites/default/files/Filtering/Monitoring/Lightspeed_Appropriate_filtering.pdf

Appendices

Appendix 1

Academy Council Terms of Reference

1. Purpose

To provide a consultative group that has wide representation from Corsham Regis pupils, with some responsibility for issues regarding online safety and the monitoring of the online safety policy including the impact of initiatives.

2. Membership

2.1. The Academy Council will seek to include representation from all stakeholders.

The composition of the group should include:

- Headteacher
- Governor responsible for online safety - when appropriate
- pupil representation – for advice and feedback.

2.2. Other people may be invited to attend the meetings at the request of the Headteacher on behalf of the committee to provide advice and assistance where necessary.

3. Chairperson

The Headteacher is the Chairperson. Their responsibilities include:

- Scheduling meetings and notifying committee members;
- Inviting other people to attend meetings when required by the committee;
- Guiding the meeting according to the agenda and time available;
- Ensuring all discussion items end with a decision, action or definite outcome;
- Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

4. Duration of Meetings

Meetings shall be held termly for a period of half an hour. A special or extraordinary meeting may be called when and if deemed necessary.

5. Functions

These are to assist the Headteacher with Online Safety responsibilities with the following:

- To keep up to date with new developments in the area of online safety
- To (at least) annually review and develop the online safety policy in line with new technologies and incidents
- To monitor the delivery and impact of the online safety policy
- To monitor the log of reported online safety incidents (anonymous) to inform future areas of teaching / learning / training.
- To co-ordinate consultation with the whole school community to ensure stakeholders are up to date with information, training and/or developments in the area of online safety. This could be carried out through:
    - Staff meetings
    - Pupil forums (for advice and feedback)
    - Governors meetings
    - Surveys for pupils, parents / carers and staff

- Parents evenings
- Website/Newsletters
- Online safety events
- Internet Safety Day
- Other methods

- To monitor incidents involving cyberbullying for staff and pupils

Links to other organisations or documents

UK Safer Internet Centre

Safer Internet Centre – http://saferinternet.org.uk/
South West Grid for Learning - http://swgfl.org.uk/
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/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

INSAFE - http://www.saferinternet.org/ww/en/pub/insafe/index.htm
UK Council for Child Internet Safety (UKCCIS) - www.education.gov.uk/ukccis
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/

Bullying / Cyberbullying

DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – new Cyberbullying guidance and toolkit (Launch spring / summer 2016) -
http://www.childnet.com/new-for-schools/cyberbullying-events/childnets-upcoming-cyberbullying-work
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people
Connectsafely Parents Guide to Facebook
Facebook Guide for Educators

- Curriculum

SWGfL Digital Literacy & Citizenship curriculum
Glow - http://www.educationscotland.gov.uk/usingglowandict/
Teach Today – www.teachtoday.eu/
Insafe - Education Resources
https://www.gov.uk/government/publications/education-for-a-connected-world

- Data Protection

Information Commissioners Office:

Your rights to your information – Resources for Schools - ICO
Guide to Data Protection Act - Information Commissioners Office
Guide to the Freedom of Information Act - Information Commissioners Office
ICO guidance on the Freedom of Information Model Publication Scheme
ICO Freedom of Information Model Publication Scheme Template for schools (England)
ICO - Guidance we gave to schools - September 2012 (England)
ICO Guidance on Bring Your Own Device
ICO Guidance on Cloud Hosted Services
Information Commissioners Office good practice note on taking photos in schools
ICO Guidance Data Protection Practical Guide to IT Security
ICO – Think Privacy Toolkit
ICO – Personal Information Online – Code of Practice
ICO Subject Access Code of Practice
ICO – Guidance on Data Security Breach Management
NEN - Guidance Note - Protecting School Data

- Professional Standards / Staff Training

DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs
Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs
UK Safer Internet Centre Professionals Online Safety Helpline

Appendix 2:

Online Safety curriculum at Corsham Regis Primary Academy

The National Curriculum and Online Safety

The Computing curriculum started from September 2014 when the new national curriculum was published. In terms of teaching Online Safety to pupils, this document says:

'Aims:

The national curriculum for computing aims to ensure that all pupils:

- are responsible, competent, confident and creative users of information and communication technology.

At Key Stage 1
Pupils should be taught to:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Teaching resources to achieve this (Click here)

- Safety: SMART Rules, Safer Internet Day, Zippep's Astro Circus
- Respectfully: Digiduck's Big Decision (Childnet), SMART Rules, Safer Internet Day , Lee and Kim (CEOP Think You Know), Zippep's Astro Circus
- Keeping Personal Information Private: SMART Rules, Hector's World (CEOP), Lee and Kim (CEOP), Zippep's Astro Circus
- Help and Support: Smartie the Penguin, Hector's World (CEOP), Zippep's Astro Circus
- Content: SMART Rules and Magda and Mo – The Pirate's Donut
- Contact: SMART Rules, Hector's World (CEOP), Lee and Kim (CEOP)

At Key Stage 2
Pupils should be taught to:

- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Teaching resources to achieve this (Click here):

- Search technologies: SMART Rules, Safe Search Lesson Plan (KidSMART)
- Safety: SMART Rules, Safer Internet Day, Cybersmart Access, Comic Book Capers (Cybersmart), Play Like Share https://www.thinkuknow.co.uk/teachers/
- Respectfully: SMART Rules, Safer Internet Day, Cyber Café, Beaker You Choose (BBC), Digital Literacy Curriculum http://www.digital-literacy.org.uk/Home.aspx
- Responsibly: Only a game (Childnet)
- Personal Information: SMART Rules, Horrible Histories (Guy Fawkes – Internet Privacy Settings), Information Commissioners Office
- Behaviour: BrainPOP, Horrible Histories (Saxon Monk – Internet Videos are Forever)
- Cyber bullying: SMART Rules, BeatBullying
- Reporting: Child Exploitation and Online Protection (CEOP) – Think You Know, Safer Internet Day, Childnet skills school, Childline
- Content: SMART Rules, Horrible Histories (Lady Jane Grey – Beware of What You Download & Prudish Victorian – Don't Lie About Your Age Online), Digital Adwise (Media Smart)
- Contact: SMART Rules, Jigsaw (CEOP), Cybersmart Access

Internet safety is included in the Programmes of Study for all Key Stages to help ensure that young people are "responsible, competent, confident and creative users of information and communication technology."

Internet Safety in Learn for Life (PSHE) and Sex & Relationships Education

Internet safety is not just restricted to the Computing curriculum. Learn for Life (PSHE) and Sex & Relationships Education provide great opportunities for approaching a range of key internet safety issues such as cyberbullying, safe social networking, healthy digital behaviours, pornography, sexting, privacy and online reputation.

While PSHE education is a non-statutory subject, section 2.5 of the National Curriculum framework document states that:

'All schools should make provision for PSHE, drawing on good practice.'

Along with the National Curriculum framework, the DfE also published guidance on PSHE education, which states that the subject is 'an important and necessary part of all pupils' education' and that:

'Schools should seek to use PSHE education to build, where appropriate, on the statutory content already outlined in the national curriculum, the basic school curriculum and in statutory guidance on: drug education, financial education, **sex and relationship education** (SRE) and the importance of physical activity and diet for a **healthy lifestyle**.'

Section 2.1 of the National Curriculum framework states:

'Every state-funded school must offer a curriculum which is balanced and broadly based and which:
· promotes the spiritual, moral, cultural, mental and physical development of pupils at the school and of society
*· prepares pupils at the school for the opportunities**, responsibilities and experiences of later life'***

These duties are set out in the 2002 Education Act (the 2010 Academies Act also refers to the broad and balanced curriculum). Schools also have statutory responsibilities in relation to promoting pupil wellbeing and pupil safeguarding (Children Act 2004) and community cohesion (Education Act 2006). The Equality Act 2010 also places duties on schools to help to reduce prejudice-based bullying and in doing so to keep protected characteristic groups safe. PSHE education plays an important part in fulfilling all of the responsibilities.

All schools have responsibilities relating to the safety of children in their care - see **Keeping Children Safe in Education September 2018**, the Department for Education states:

Additional resources:

- Childnet's resource bank can also be sorted by Key Stage and topic.
- Childnet has also created a resource, E-Safety in the Computing Curriculum, with guides for KS1 and 2 to highlight the key learning aims related to E-Safety in the Computing curriculum and signpost to some key resources that can be used in the classroom to help deliver these aims.
- The Sex Education Forum's magazine also has a Pornography Issue which discusses how to approach issues surrounding pornography in school.

	Autumn	Spring	Summer
	Term 1/2	**Term 3/4**	**Term 5/6**
Whole School Computing theme	Digital Literacy: Communication & Collaboration / Understanding networks	Information Technology: Digital Research / Safety & Security	Computer Science: Digital Content-Multimedia / Programming & Coding
KS1 Online Safety themes	Safety Respect Keeping Personal Information Private Contact Help and Support	Safety Keeping Personal Information Private Help and Support Content Contact	Safety Respect Content Contact
KS2 Online Safety themes	Search technologies Safety Respect Being responsible Personal Information Acceptable / Unacceptable Behaviour Cyber bullying Reporting Content Contact	Search technologies Safety Respect Being responsible Personal Information Acceptable / Unacceptable Behaviour Reporting Content Contact	Search technologies Safety Being responsible Reporting Content Contact

Curriculum overview for Online Safety

Appendix 3i: Pupil Acceptable Use Agreement for Foundation Stage and Key Stage 1

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 will only take photographs of other children or adults if I ask them and they say that it's ok

• I will only use a school computer / tablet in school

• I will not change the settings on a school computer / tablet

• I will not bring into school a mobile phone or my own tablet unless my teacher says that I can. If I do, I understand that the school is not responsible if it is lost, stolen or broken

• I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child):

Signed (parent):

These rules help us to be fair to others and keep everyone safe.

Appendix 3ii: Pupil Acceptable Use Agreement for Key Stage 2

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 Corsham Regis 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, tell my parents 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 Corsham Regis 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 Corsham Regis 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.

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 photographs, videos or images of other pupils or staff without their permission.
- I will not distribute any photographs, videos or images of other pupils or staff 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 academy:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission from the Headteacher. I understand that, if I do use my own devices in the academy, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- If I do bring into school a mobile phone or my own tablet – without or without permission of the Headteacher, I understand that the school is not responsible if it is lost, stolen, broken or damaged in some way
- 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 or tablet settings.
- I will not use social media sites at school

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 Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

My name is:

My class teacher is:

Signed: Date:

The academy may exercise its right to monitor the use of the academy's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the academy's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. Talkstraight monitors all internet use and will notify the police and Local Authority if an illegal website is accessed.

Appendix 4: Parent / Carer ICT Acceptable Use Agreement

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

This ICT Acceptable Use Agreement is intended to ensure:

- All young people will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- Academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Personal data of pupils, parents, staff and governors is kept secure
- Parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their online behaviour.

Corsham Regis Primary Academy will try to ensure that children have good access to ICT to enhance their learning and will, in return, expect the children to agree to be responsible users. A copy of the Pupil Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the academy's expectations of the young people in their care.

Parents are requested to sign the permission form below, to show their support of the academy in this important aspect of its work.

As the parent/carer of the pupil/s, I give permission for my child/children to have access to the internet and to ICT systems in school.

I know that my child/children has/have signed an Acceptable Use Agreement and has/have received, or will receive, Online Safety education to help them understand the importance of safe use of ICT both in and out of school.

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

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

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

I understand that Corsham Regis Primary Academy accepts no liability in respect of any loss/damage to personal ICT devices while at school or in transit. The decision to bring a personal ICT device into school rests with the pupil and the parent/carer, as does the liability for any loss/damage that may result from the use of a personal ICT device in school.

Use of Digital / Video Images

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

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

The academy will comply with the Data Protection Act and request parents / carers permission before taking images of members of the academy. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act) unless specifically asked not to, ie during our Someone Special Days. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree
Please complete and return this slip to Mrs Hunt in the main office.
Thank you
Mrs Abby Symons
Headteacher

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

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

I have read and understood the Pupil Acceptable Use Agreement for my son/daughter and agree to support it.

Name of pupil: Name of parent(s):

Signed: Date:

Appendix 5: Acceptable Use Agreement for all Corsham Regis Primary Academy Staff

Corsham Regis Primary Academy, as part of The Corsham School Academy Group, is committed to provide the best ICT infrastructure it can to support the highest standards of teaching and learning, and the highest standards of support and the efficient running of all school business. All staff must however accept that their use of these resources is for professional purposes only and use must comply with legal, moral and safety codes, including child protection and data protection. The Corsham School (ICT) Acceptable Use Policy (part of the Personnel Policy) sets out the rules and guidelines for all staff (Please refer to this policy for further guidance).

This policy relates to teachers' standards:
9. Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by:
9.2 Having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions.

The principles of this policy are:
• Staff have a personal responsibility in all matters of school computer use.
• Staff have access to computer equipment to carry out their specified roles, which includes access to email.
• Staff have a duty to protect students and other staff from undesirable information, particularly accessed through the internet.
• Use of school computer equipment must comply with the Data Protection Act, and the Misuse of Computers Act. See Appendices 1 & 2 of The Corsham School (ICT) Acceptable Use Policy (part of the Personnel Policy).

In addition to the requirements of The Corsham School (ICT) Acceptable Use Policy (part of the Personnel Policy), all staff at Corsham Regis understand that new technologies have become integral to the lives of children and young people in today's society, both within school 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 Agreement is intended to ensure:

- that staff 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 personal data of pupils, parents, staff and governors is kept secure
- that staff are protected from potential risk in their use of technology in their everyday work.

Corsham Regis will try to ensure that staff have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff to agree to be responsible users.

Acceptable Use 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. I know the importance of keeping personal data safe and will comply with the Data Protection Policy for The Corsham School Academy Group. 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 school 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, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use, not for personal or recreational use
- 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 report any breach of an individual's personal data to the Data Controller

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 school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the school website) 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 school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school 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.

Corsham Regis and The Corsham School Academy Group 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 school, 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
- 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 Corsham School Academy Group Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted and password protected. 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 school 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 Agreement applies not only to my work and use of academy digital technology equipment in school, 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 Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and, in the event of illegal activities, the involvement of the police.

At Corsham Regis Primary Academy I will use academy ICT systems and hardware responsibly and keep personal data secure by:

- Recognising all IT remains the property of Corsham Regis Primary Academy.
- Understanding that if IT hardware is allocated to a named member of staff, it is their responsibility. If another member of staff borrows it, the responsibility still stays with the staff member allocated. Only Corsham Regis Primary Academy staff should use the IT hardware.
- Keeping the school IT hardware on site at all times.
- Returning the school's IT hardware to the Admin and Finance manager for re-allocation on leaving the academy's employment.
- Reporting any lost or stolen device immediately
- Switching off the IT hardware not being used at the end of each working day, and locking away it away over the weekend and during school holidays.
- Locking the screen on the IT hardware when away from the device and not able to supervise its usage
- Checking installed virus protection software on the device is kept up to date.
- Not attempting to alter the computer settings other than to personalise the desktop working area.
- Reporting any fault which occurs with the IT hardware immediately to MARCSS, via the online reporting system.
- Using a strong password or pin to secure all devices, including personal devices if these are used to access or download school communications
- Logging out of any websites or applications which contain personal or sensitive information after use
- Using encryption to store data on a device securely
- Saving documents which include personal data in a secure folder on the server and not on the desktop or local drive
- Password protecting all documents including personal or sensitive data
- Printing off documents which include personal or sensitive data to a secure school printer only, and that this is locked securely away in school when it is not in use or shredded if finished with
- Locking away hard copies of personal / sensitive data in school
- Not sharing passwords for documents and websites with others
- Not use personal email accounts for any school related communications
- Keeping individual logins to electronic devices private and not recorded in locations where they could be discovered by others
- Securing data on all devices at home by creating separate logins for other family users
- Transferring documents between home and school which include personal / sensitive information using an encrypted USB stick provided by Corsham Regis or using OneDrive through your school Office 365 account
- Checking that the encrypted USB stick has been registered with the Admin and Finance Manager, Mrs Tracie Brewer, and returning it when leaving employment of The Corsham School Academy Group
- Not using public cloud-based sharing and public backup services
- Not downloading untrusted or unverified apps

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

Staff Name: .....

Signed: .....

Date: .....

Appendix 6: Acceptable Use Agreement for all Corsham Regis Primary Academy Governors

Corsham Regis Primary Academy, as part of The Corsham School Academy Group, is committed to provide the best ICT infrastructure it can to support the highest standards of teaching and learning, and the highest standards of support and the efficient running of all school business. All governors must however accept that their use of these resources is for professional purposes only and use must comply with legal, moral and safety codes, including child protection.

All governors at Corsham Regis understand that new technologies have become integral to the lives of children and young people in today's society, both within school 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 governors 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 Agreement is intended to ensure:

- that governors 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 personal data of pupils, parents, staff and governors is kept secure

Acceptable Use Agreement

I understand that I must use IT 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 professional and personal safety:

- I understand that the academy will monitor my use of the school 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, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use, not for personal or recreational use
- 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 report any breach of an individual's personal data to the Data Controller (Mr Gareth Spicer, the Headteacher)

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 school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the school website) 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 school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my role or responsibilities as governor.

Corsham Regis and The Corsham School Academy Group 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 school, 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 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
- 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 Corsham School Academy Group Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted and password protected. Paper based protected and restricted data must be held in lockable storage.

- I understand that The Corsham School Academy Group 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 school 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 school, but also applies to my use of academy systems.
- 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 / Directors and, in the event of illegal activities, the involvement of the police.

At Corsham Regis Primary Academy I will use academy ICT systems and hardware responsibly and keep personal data secure by:

- Recognising all IT remains the property of Corsham Regis Primary Academy.
- Keeping the school IT hardware on site at all times.
- Reporting any lost or stolen device immediately
- Locking the screen on the IT hardware when away from the device and not able to supervise its usage
- Checking installed virus protection software on the device is kept up to date.
- Using a strong password or pin to secure all devices, including personal devices if these are used to access or download school communications
- Logging out of any websites or applications which contain personal or sensitive information after use
- Using encryption to store data on a device securely
- Password protecting all documents including personal or sensitive data
- Printing off documents which include personal or sensitive data to a secure school printer only, and that this is locked securely away in school when it is not in use or shredded if finished with
- Locking away hard copies of personal / sensitive data in school
- Not sharing passwords for documents and websites with others
- Keeping individual logins to electronic devices private and not recorded in locations where they could be discovered by others
- Not use personal email accounts for any school related communications
- Securing data on all devices at home by creating separate logins for other family users
- Transferring documents between home and school which include personal / sensitive information using an encrypted USB stick provided by Corsham Regis or using OneDrive through your school Office 365 account
- Checking that the encrypted USB stick has been registered with the Admin and Finance Manager, Mrs Tracie Brewer, and returning it when leaving employment of The Corsham School Academy Group

- Not using public cloud-based sharing and public backup services
- Not downloading untrusted or unverified apps

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

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

Staff Name: .....

Signed: .....

Date: .....

Appendix 6: Responding to Sexting

Appendix 8: Online Safety incident log sheet

Date of alleged		**Date/time of disclosure**	

incident			
Name of child/ren / adult / staff member		**Class / contact details of those involved**	
Name of person making this record		**Role in school**	
Signed as a true record		**Date DD/MM/YY**	
Location of where incident took place			
Details of what happened: (include the actual words spoken by the child where possible)			

Nature of incident	☐ Bullying or harassment ☐ Online bullying or harassment (cyberbullying) ☐ Sexting (self-taken indecent imagery) ☐ Deliberately bypassing security or access ☐ Hacking or virus propagation ☐ Racist, sexist, homophobic, religious hate material ☐ Terrorist material ☐ other (please specify)_____			
	Deliberate access	Yes / No	**Accidental access**	Yes / No
Did the incident involve material being	☐ created ☐ viewed ☐ printed ☐ shown to others ☐ transmitted to others			

	☐ distributed
Action taken	**Staff** ☐ incident reported to HT/DSL ☐ advice sought from the MASH ☐ incident reported to police ☐ incident reported to CEOP ☐ incident reported to Internet Watch Foundation ☐ incident reported to IT ☐ disciplinary action to be taken ☐ E-Safety policy to be reviewed / amended **Child/young person** ☐ incident reported to member of staff (specify) _____ ☐ incident reported to social networking site ☐ child's parents informed ☐ incident reported to IT ☐ disciplinary action to be taken ☐ child/young person debriefed ☐ E-Safety policy to be reviewed / amended
Name of Designated Safeguarding Lead reviewing the concern	

Outcome of incident / investigation			
Children's social care:			
Police / CEOP:			
Organisation:			
Individual (staff member / child):			
Other (HR/legal etc)			
Further action taken **Please also record whether concerns were shared with:** • **parents/carers** • **MASH** **and reason(s) why:**		**Date**	
Learning from the case			

Key learning point 1		
Key learning point 2		
Key learning point 3		
Recommendations		**Timescale to be implemented**
Recommendation 1		
Recommendation 2		
Recommendation 3		