CHADSGROVE SCHOOL

ONLINE SAFETY AND ACCEPTABLE USE POLICY

April 2021

Policy No: 87

DATE APPROVED BY GOVERNING BODY: 26.4.2021

DATE OF NEXT REVIEW: Spring 2024

Lead: Angela Macvie

Governor Responsible: Governing Body

CONTENTS

Online Safety and Acceptable Use Policy Details

Online Safety Lead: Mrs Angela Macvie

Designated Safeguarding Lead: Ms Deb Rattley

GetSafe Lead: Mrs Angela Macvie

Learning Platform Lead: Mrs Angela Macvie

Ratified by Governing Body on:

Next review date:

1. Introduction

1.1. Chadsgrove School embraces the positive impact and educational benefits that can be achieved through the appropriate use of the Internet and associated communications technologies.

1.2. Chadsgrove is also aware that inappropriate or misguided use can expose both adults and young people to unacceptable risks and dangers. To that end, the school aims to provide a safe and secure environment which not only protects the school community but also educates them on how to stay safe in the online world.

1.3. The policy has been developed in consultation with the Senior Leadership Team and Governing Body.

2. Scope

2.1. This policy and related documents apply at all times to both fixed and mobile technologies owned and supplied by the school and to personal devices owned by adults or pupils and used whilst on the school premises.

2.2. Where possible, this policy has been explained to the pupils of the school so that they:

- Understand that there are dangers associated with the Internet and associated mobile technologies
- Know what behaviour is expected of them
- Know what to do if they encounter unacceptable, undesirable or inappropriate use of technology

3. Illegal, Undesirable or Inappropriate Activities

3.1. Chadsgrove School believes that the following activities are illegal, undesirable or inappropriate and that users should not engage in them when using school equipment or systems both in and out of school:

- Visiting internet sites, making, posting, downloading, uploading, transferring, communicating or passing on, material, remarks, proposals or comments that contain or relate to:
    - Child sexual abuse images (illegal – The Protection of Children Act 1978)
    - Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
    - Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
    - Criminally racist material in UK – to stir up religious hatred or hatred on the grounds of sexual orientation (illegal – Public Order Act 1986)
    - Pornography
    - Promotion of any kind of discrimination
    - Promotion of racial or religious hatred
    - Threatening behaviour, including promotion of physical violence or mental harm
    - Any other information which may be offensive, breaches the integrity of the ethos of the school or brings the school into disrepute

- Running a private business

- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school

- Uploading, downloading or transmitting commercial software or any other copyrighted materials belonging to third parties, without the necessary licensing permissions

- Creating or propagating computer viruses or other harmful files

- Carrying out sustained or instantaneous high volume network traffic (downloading or uploading files) that causes network congestion and hinders others in their use of the internet

- On-line gambling and non-educational gaming

- Publicly criticising or blaming school management, colleagues, Worcestershire Children First or the county council through any medium including internet 'blogs', websites or social networking tools

- Disclosing or publicising any confidential or personal information about the school, its staff, pupils or other members of the school community

- Using social media in any way that might bring the school into disrepute or undermine its' policies or ethos

4. Roles and Responsibilities

4.1. The Governing Body

- Is responsible for the approval of this policy and for reviewing its effectiveness by receiving regular information about online incidents and monitoring reports

4.2. The Head Teacher

- Has ultimate responsibility for establishing safe practice and managing online issues at Chadsgrove. The Head Teacher, in turn, delegates responsibility for the day to day management of online safety issues to the Online Safety lead
- Is responsible for ensuring that she is familiar with the procedures to be followed in the event of a serious online allegation being made against a member of staff
- Ensures that the Online Safety Lead receives appropriate training and support to fulfil their role effectively

4.3. The Online Safety Lead

- Enables all staff to take day to day responsibility for online safety issues by providing systems and information that enable them to contribute to the monitoring of ICT use in the school
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Has a leading role in establishing and reviewing the school online safety policy
- Provides advice and access to training for staff
- Liaises with the Local Authority as necessary
- Liaises with the school ICT and Computing Team
- Reviews, at least weekly, the output from monitoring software and initiates action when necessary
- Meets regularly with the Head Teacher to discuss current issues and any incident logs
- Attends relevant meetings of the Governing Body when requested to do so

4.4. School Staff

- Safeguard the welfare of children and refer any concerns to the Designated Safeguarding Lead
- Have an up to date awareness of online matters and of the current school online safety policy and practices
- Use technology responsibly and in line with this policy

- Read, understand and sign the school's Acceptable Use Agreement for staff
- Accept responsibility for their use of technology
- Report any suspected misuse, incidents or problems to the Online Safety Lead or a member of the Senior Leadership Team
- Embed online safety issues in the curriculum and other school activities
- Understand that all network activity and online communications are monitored and be aware that in certain circumstances, where unacceptable use is suspected, enhanced monitoring and procedures may come into action
- Model best practice and the appropriate use of school resources, including the internet, at all times

4.5. ICT technician (Service Level Agreement held with Netbuilder)

- Ensures the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- Ensures any shortcomings in the infrastructure are reported to the Online Safety Lead or Head Teacher so that appropriate action may be taken
- Ensures the school meets current online safety technical requirements
- Ensures users only access the school's networks through password protected means

5. Acceptable Use Policy Agreements

5.1. All members of the school community are responsible for using the school ICT systems (or their own personal devices on the school site) in accordance with the appropriate Acceptable Use Policy, which they will be expected to sign before being given access to school systems.

5.2. Acceptable use policy agreements are provided for:

- Pupils (where it is appropriate)
- Staff
- Volunteers
- Visitors / Community users

5.3. All employees of the school and volunteers sign a written Acceptable Use Policy Agreement when they take up their role in school and if significant changes are made to the policy.

5.4. Visitors / community users sign when they first request access to the school's ICT system. This is then valid for any future visits, unless any significant changes are made to the policy.

5.5. Pupils with severe or profound and multiple learning difficulties, who are unable to independently access the internet or mobile technologies are not required to sign an Acceptable Use Policy Agreement.

5.6. With the exception of pupils with severe or profound and multiple learning difficulties, all users are required to agree to an Acceptable Use Policy before being allowed to log on to the school network. Wherever possible, the Acceptable Use Policy will be explained to pupils at a developmentally appropriate level.

6. Internet Access

6.1. Central filtering of websites is provided and managed by Netbuilder. Staff requiring access to a restricted site are required to submit a request to Netbuilder and this will be granted or denied once the website has been reviewed.

6.2. Requests for changes to filtering are directed to the Online Safety lead in the first instance who forwards these on to Netbuilder or liaises with the Head Teacher as appropriate.

6.3. All staff and students (where appropriate) understand that if an inappropriate site is discovered it must be reported to the Online Safety lead who will report it to Netbuilder in order to be blocked.

6.4. If any incidents occur, where it is suspected that an inappropriate website has been accessed, then this will be recorded in the Online Safety log book for audit purposes.

7. Email

7.1. Access to email is provided for all users in school through Microsoft Office 365. This has been setup by Netbuilder, as a part of their broadband service, which the school uses to provide internet connectivity.

7.2. All staff and pupils (where appropriate) are provided with an email account and password set up by a member of the school ICT and Computing Team or Netbuilder. They understand that their school email account must be used for all educational and professional communications. The school encourages the use of e-mail to contact the school via the school office or staff professional e-mail addresses. The school does not publish any contact details for the pupils.

7.3. Everyone in the school community who is able to use email is informed, through the Acceptable Use Policy (and explained to pupils where appropriate), that the e-mail system may be monitored and should not be considered private communication.

7.4. Staff are allowed to access personal e-mail accounts on the school system outside of directed time and understand that any messages sent using school equipment should be in line with the Acceptable Use policy. In addition, they are made aware that these messages will be scanned by the monitoring software in place.

7.5. Pupils may be given the opportunity to check their personal or Chadsgrove e-mail outside of lesson time and understand that any messages sent using the school equipment should be in line with the Acceptable Use Policy. In addition, they are made aware that these messages will be scanned by the monitoring software.

7.6. Users must immediately report, to the Online Safety Lead or Designated Safeguarding Lead, the receipt of any email that makes them feel uncomfortable or is offensive, threatening or bullying in nature. They must not respond to such emails.

7.7. Where appropriate, pupils are made aware of the dangers and good practices associated with the use of email through the Online Safety sessions that form a part of the long-term plan for ICT and Computing.

7.8. It is recognised that e-mail or instant messages received or transmitted by pupils can contain language or content that is unacceptable. It is also recognised that some people may try to use e-mail to identify and contact pupils for unacceptable reasons. To help to avoid these problems, Smoothwall, the monitoring software that is used by Chadsgrove, monitors all messages sent or received using school-owned equipment, whether or not it is connected to the school network. It also captures all inappropriate content which can then be reviewed by authorised staff.

7.9. It is acknowledged that the Office 365 email system is web based and can be accessed by pupils at home, as can instant messaging systems and social networking sites, on machines that are not owned by school and do not have monitoring software installed on them. As such, parent carers are also encouraged to be vigilant and carefully monitor their child's use of technology. There is an online safety section on the school website to support with this.

7.10. To avoid pupils revealing their identification within e-mail messages they are taught never:

- To reveal their address
- To give information that might reveal their whereabouts
- To reveal any other personal information that may allow strangers to identify them

This message is frequently re-enforced in order to ensure that pupils retain the information and can be reminded about what to do if they have a problem.

7.11. If staff believe that pupils have been targeted with e-mail messages by parties with criminal intent, the messages will be retained, the incident recorded, and the Governors and the pupil's parent carers informed. Advice from the Local Authority will also be taken regarding any further action.

8. Chadsgrove School Website

8.1. The Chadsgrove School website can be found at https://www.chadsgroveschool.org.uk/web

8.2. Chadsgrove uses its website in order to share information with and beyond the school. This includes, from time-to-time, celebrating the work and achievements of pupils. Pupils are not identified by name on the school website. If, for any reason, a pupils' name does need to be included, only his/her first name will be used and only then following consent from the parent care. Pupil's work is only published on the school website following permission from their parent carers.

8.3. Personal information is not posted on the school website and only professional email addresses are used to identify members of staff.

8.4. The Head Teacher takes overall responsibility for content published to the school website but delegates general editorial responsibility to Angela Macvie (Online Safety Lead and Deputy Head Teacher), Justine Marson (Office Administrator) and Jacqueline Pitt (School Business Manager).

8.5. Class teachers and subject leaders are responsible for the editorial control of any work published by their pupils.

8.6. The school will hold the copyright for any material published on the school website or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

9. Chadsgrove School Learning Platform

9.1. The Chadsgrove School learning platform can be found at https://chadsgrove.eschools.co.uk/. This link is secure and password protected.

9.2. The use of the learning platform is monitored by the Online Safety lead. In addition, if the learning platform is accessed using laptops/desktops installed with the Smoothwall monitoring software, any captures that cause concern can be reviewed and acted upon if necessary by the Designated Safeguarding Lead.

9.3. The Online Safety and Learning Platform lead also monitors staff use of the learning platform and if any concerns are raised these will be raised directly with the Designated Safeguarding Lead.

9.4. User accounts and access rights can only be created by the Online Safety and Learning Platform lead and only current pupils or members of staff are able to access to the learning platform. When staff or pupils leave the school their accounts will be disabled.

9.5. Pupils are advised on acceptable conduct and use when using the learning platform prior to accessing it for the first time and are reminded about this at regular intervals, for example during online sessions that form part of the long-term plan for ICT and Computing.

9.6. Any concerns with regard to behaviour or content on the learning platform may be recorded and will be dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive
- The material will be removed by the Learning Platform lead if the user does not comply
- Access to the learning platform for the user may be suspended and the user will need to discuss the issues with the Head Teacher before reinstatement
- A pupil's parent carer will be informed

9.7. A visitor may be invited onto the learning platform by the Learning Platform lead following a request from a member of staff. In this instance, there may be an agreed focus or a limited time slot/access.

9.8. The Head Teacher takes overall responsibility for content published to the school learning platform but delegates general editorial responsibility to Angela Macvie (Online Safety and Learning Platform Lead).

9.9. Class teachers and subject leaders are responsible for the editorial control of any work published by their pupils.

9.10. The school will hold the copyright for any material published on the school learning platform or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

10. Chadsgrove School Twitter Account

10.1. Chadsgrove's Twitter account can be found at https://twitter.com/chadsgrove

10.2. Chadsgrove's Twitter account is currently accessed only by staff and administrated by Emma Nolan (TA4). Should pupils contribute to the Twitter account, this will be under the direct supervision of a member of staff.

10.3. The Online Safety lead will check/moderate any content placed onto Twitter. Any concerns will be passed directly to the Head Teacher / Designated Safeguarding Lead.

10.4. The Head Teacher takes overall responsibility for content published to the school Twitter account but delegates general editorial responsibility to Angela Macvie (Online Safety Lead and Deputy Head Teacher) and Emma Nolan (TA4).

10.5. Class teachers and subject leaders are responsible for the editorial control of any work published by their students.

10.6. The school will hold the copyright for any material published on the Twitter account or will obtain permission from the copyright holder prior to publishing with appropriate attribution.

11. Anti-Virus Software

11.1. Windows Defender is installed on all computers by Netbuilder, as part of Office 365, and is updated automatically. Any alerts are managed by Netbuilder.

12. Monitoring of the Use of Computers, Software, Email and Internet Use

12.1. Smoothwall Monitoring software is installed on all desktops and laptops that are owned by the school and connect to the school network. Smoothwall works by monitoring all computer activity and generating screen captures of any activity that contains a trigger word from one of its many libraries. The screen captures are stored centrally on a server hosted by Smoothwall. Smoothwall continues to work when laptops are used off site, capturing screen shots and forwarding these to the Smoothwall servers using any wifi connection.

12.2. Reporting functions within Smoothwall provide information that can be used both to identify any inappropriate use of computers and also to identify vulnerable young people (or staff) who may be suffering from modern day life pressures including, but not limited to, abuse, bullying, anxiety, and depression disorders.

12.3. Monitoring of staff and pupil behaviour using Smoothwall is carried out, on a regular basis, by the Online Safety Lead or Designated Safeguarding Lead. In addition, the software generates an email to the Online Safety Lead if a certain threshold number of captures for any particular individual or computer is reached. Should this occur, Smoothwall is accessed, as soon as possible, in order to investigate any potential issues.

13. School Network Access

13.1. All staff are issued with their own username and password in order to access the school network.

13.2. Visitors or supply staff are issued with a visitor ID and have only restricted access to the school network.

13.3. All pupils use class logon ID's for their network access and then store their work in a named folder within this. Some individual pupils have their own ID's, for various reasons. Such IDs are created in exactly the same way and have the same restrictions placed upon them as class logons.

14. Access to Undesirable Materials by Pupils

14.1. Pupils at Chadsgrove who are cognitively able to perform internet searches are taught that they must never intentionally seek offensive material on the Internet. Any transgression is likely to be captured by Smoothwall but staff witnessing this behaviour should notify the Online Safety Lead or Head Teacher immediately. Any incident will be treated as a disciplinary matter, and the parent carers of the pupil involved will normally be informed. The incident will be recorded in the Online Safety log.

14.2. If deliberate access to undesirable materials it repeated, flagrant or habitual, the matter will be treated as a serious disciplinary issue. The pupil's parent carers will be informed and the Governing Body will be advised.

14.3. Unintentional access of undesirable materials, for example when a web search yields unexpected results should also be picked up by Smoothwall but, again, should be reported to the Head Teacher or Online Safety Lead if it is observed by a member of staff and recorded in the Online Safety Log.

15. Deliberate Access to Undesirable Materials by Adults

15.1. Deliberate access to undesirable materials by adults is unacceptable and will be treated as a disciplinary issue. The Governors will be advised and the Local Authority will be consulted.

16. Mobile Technologies

16.1. Teaching staff and Senior Teaching Assistants at Chadsgrove are provided with a laptop for educational use and their own professional development. They may also be provided with an iPad or a mobile phone. All staff understand that the acceptable use policies apply to any equipment that they are issued with and sign an agreement to this fact prior to taking ownership of it.

16.2. To ensure the security of the school systems, personal equipment is currently not permitted to be connected to the school network, unless this has been authorised by the Head Teacher or Online Safety Lead and up to date virus software is installed where necessary.

16.3. Staff understand that they should use their own mobile phones sensibly and in line with school policy. Where pupils are able to use mobile phones, they are encouraged to understand that their mobile phones must be turned off during directed time and used in line with school policies at all other times.

16.4. The Educations and Inspections Act 2006 grants the Head Teacher the legal power to confiscate mobile devices where there is reasonable suspicion of misuse and the Head Teacher will exercise this right at her discretion.

16.5. Images of staff and pupils are not to be taken on personal devices unless permission has been granted to do so by a member of the Senior Leadership Team. Any images must be transferred to the school network at the earliest convenience.

16.6. New technologies are evaluated and risk assessed for their educational benefits before they are introduced to the school community.

17. Digital Media and the Use of 'Zoom'

17.1. Chadsgrove School respects the privacy of the school community and will obtain written permission from staff, parent carers or pupils before any images, video or sound recordings are published or distributed outside of the school. In addition to this:

- Photographs will not identify any individual pupil
- Pupils' full names will not be published outside of the school environment

17.2. If external video conferencing / 'Zoom' calls occur, then this will be fully supervised by school staff at all times.

17.3. School staff are requested to follow the following guidelines with regard to the use of 'Zoom' and other such video conferencing applications: Use a new meeting room each time (ie. don't use the personal meeting ID)

- Don't allow attendees to join before the host
- Mute attendees on joining
- Turn screen sharing off and grant access only as it is required
- Set up a 'waiting room'
- Lock your meeting room after you have started
- Don't publicise the meeting's link on social media
- Don't publically share the screenshot of everyone, especially when it shows the meeting ID
- Try to have someone who's job it is to 'manage the room' and focus just on doing that.
- Tell people what the Plan B is (for example, if the meeting has to be aborted)

17.4. Additionally, staff are requested to

- Avoid sharing personal information
- Turn off microphones, unless they are needed
- Ensure that two members of staff are present in all meetings that involve pupils

18. Social Networking

18.1. The school has reviewed the use of social networking sites and currently does not allow access to sites such as Facebook. Even so, where appropriate, guidance is provided to the school community on how to use these sites safely and appropriately. This includes:

- Not publishing personal information
- Not publishing information relating to the school community
- How to set appropriate privacy settings
- How to report issues or inappropriate content

18.2. Un-moderated chat sites present an unacceptable level of risk and are blocked in school. Pupils are given age appropriate advice and guidance around the use of such sites.

19. Copyright

19.1. It is recognised that much material on the Internet is copyright, unless this is specifically waived. It is the school's policy that the copyright of Internet materials will be respected.

19.2. Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third-party materials contained within them.

20. Online Safety Training

20.1. All staff are expected to complete an online E-Safety training module. In addition:

- There is an induction process and mentor scheme available for new members of staff
- Educational resources are reviewed by subject leaders and disseminated through curriculum meetings / staff meetings / training sessions

- Online safety is embedded throughout the school curriculum and visited by each class where this is appropriate
- Where appropriate, pupils are taught how to validate the accuracy of information found on the internet
- Online advice is provided to parent carers via the school website

21. Online Safety Education

21.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. Wherever appropriate, the education of pupils in online safety is an essential part of the school's provision.

21.2. Pupils need the help and support of the school to recognise and avoid online risks and to build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them. They need to be taught how to behave appropriately when accessing the internet and on-line facilities and what to do if they encounter offensive, abusive or upsetting materials.

21.3. Online safety education is incorporated into the Long Term plan for ICT and Computing and pupils are taught the principles contained within the SMART rules in order to help to keep themselves safe:

- S – Staying SAFE by not revealing personal information
- M – The dangers of MEETING on-line friends
- A – The dangers of ACCEPTING emails from strangers, viruses in attachments etc.
- R – Pupils deciding if information is RELIABLE and understanding that people may not be truthful
- T – The need to TELL an adult if they are worried or concerned

21.4. Online safety education at Chadsgrove School includes:

- A planned online programme provided as part of the ICT and Computing and PHSE curriculum as well as assemblies and pastoral activities.
- The use of online resources such as, but not limited to
  - South West Grid for Learning
  - Childnet.com
  - Saferinternet.org
  - CEOP's Think U Know website
  - BBC Own It website
  - CEOP You Tube videos

21.5. Where appropriate, pupils are helped to understand the need for the Acceptable Use Policy Agreement and encouraged to adopt safe and responsible use of ICT both within and outside of school.

21.6. 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.

21.7. Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit, encouraging them to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.

21.8. Pupils are made aware of what to do should they experience anything, while on the internet, which makes them feel uncomfortable.

22. The School Online Safety Self Review Tool

22.1. Chadsgrove School is enrolled in the 360 degree safe 'School E-Safety Review Tool' and progression through the tool is monitored by the Online Safety Lead. This tool enables the school to review current practice over four main elements namely:

- Policy and Leadership
- Infrastructure
- Education
- Standards and Inspection

23. Publicising Online Safety

23.1. Effective communication across the school community is key to achieving the school vision for safe and responsible citizens.

23.2. In order to publicise the online safety message, Chadsgrove School will:

- Make this policy, and related documents, available on the school website
- Introduce this policy and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated
- Post relevant online safety information across school
- Provide online safety information to parents via the school website

23.3. It is important to ensure that parents are helped to keep their children safe on-line when they are at home and, as such, they are informed about the information available on the school website and advised to consult this or to speak to school staff if they require any further information or advice.

24. Data Security / Data Protection

24.1. Chadsgrove School has a duty to ensure that personal data will be recorded, processed, transferred and made available in line with the Freedom of Information Act 2000, the UK General Data Protection Regulations (GDPR) and the Data Protection Act 2018. Chadsgrove School also has a responsibility to ensure that ICT systems (and the information stored within them, even if this data is not classed as personal) are kept safe and secure.

24.2. Several documents are available that deal with the school's responsibilities with regard to data protection and security and these should be read in conjunction with this Online policy. These documents are:

- Chadsgrove School Data Protection Policy, October 2020
- Chadsgrove School Freedom of Information Policy, September 2020
- Chadsgrove School Systems and Data Security Policy, March 2020

25. Responding to Incidents

25.1. Inappropriate use of the school resources will be dealt with in line with other school policies, for example the Behaviour, Anti-Bullying and Safeguarding Policies and these should also be consulted for further information. Specifically with regard to incidents concerning ICT:

- Any suspected illegal activity will be reported directly to the police
- Third party complaints, or from parent carers, concerning activity that occurs outside the normal school day, will be referred directly to the Head Teacher
- Breaches of online policy by staff will be investigated by the Head Teacher and appropriate action will be taken under Worcestershire Children First's disciplinary procedures where a breach of any professional conduct is identified
- Pupil policy breaches relating to bullying, drugs misuse, abuse and suicide will be reported to the Designated Safeguarding Lead and action taken in line with school anti-bullying and safeguarding policies. There may be occasions when the police must be involved
- Other breaches of this policy by students will be treated as any other breach of conduct in line with the school behaviour policy

- Minor student offences, such as being off-task visiting games or email websites will be handled by the teacher in-situ using the guidance contained within the School Behaviour policy

25.2. The Educations and Inspections Act 2006 grants the Head Teacher the legal power to take action against incidents affecting the school that occur outside the normal school day and this right will be exercised where it is considered appropriate.

26. Professional Standards for Staff Communication

26.1. In all aspects of their work in our school, teachers abide by the Teachers' Standards. Teachers translate these standards appropriately for all matters relating to online.

26.2. Any digital communication between staff and pupils or parent carers:

- Must be professional in tone and content
- Must only take place on official (monitored) school systems - personal email addresses, text messaging or public chat / social networking technology must not be used for such communications

26.3. Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice as do any views and experiences of the pupils.

27. Acknowledgements

27.1. Material in this document is adapted from Online advice authored by

- Worcestershire County Council
- Birmingham City Council
- WMnet
- The South West Grid for Learning

27.2. Original copyright is held by their relevant authors and their use is gratefully acknowledged.

28. Linked Policies

- ICT and Computing (Policy Number 5)
- Pupil Behaviour (Policy Number 56)
- Safeguarding and Child Protection (Policy Number 73)
- Freedom of Information (Policy Number 86)
- Data Protection (Policy Number 84)
- School Systems and Data Security (Policy Number 85)
- Freedom of Information (Policy Number 86)
- Staff Code of Conduct (Policy Number 100)

APPENDICES

1. Acceptable use policy Agreement for Pupils on the Semi-Formal Curriculum Pathway

2. Acceptable use policy Agreement for Pupils on the Formal Curriculum Pathway

3. Acceptable use policy Agreement for Staff and Volunteers

4. Acceptable use policy Agreement for Visitors/Community Users

Acceptable use Policy Agreement

Pupils on the Semi-Formal Curriculum Pathway

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- I will only use activities on the computer if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will turn off the monitor and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
or Parent carer signature:	
Date:	

Acceptable Use Policy Agreement

Pupils Working Within the Formal Curriculum Pathway

I understand that while I am a member of Chadsgrove School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my own personal information safe as well as that of others.
- I will tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Acceptable Use Policy Agreement

Staff & Volunteers

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the online policy
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person

I will be professional in my communications and actions when using school 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 images. I will not use my personal equipment to record these images
- I will ensure that all videos/sound clips are watched in full before being used in lesson time and use the full screen view function so that advert boxes and comments are not seen
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured, unless permission has been granted to do so
- I will only communicate with pupils and parent carers using official school systems. Any such communication will be professional in tone and manner
- I will not mention the school or anything associated with it by name on social networking sites
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will not accept friend requests from children or the parents of children educated at Chadsgrove on social networking sites
- I will ensure that my personal social networking page is private

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

- I will only use my personal mobile ICT devices at school or for school related business as agreed in the online policy and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful software
- I will ensure that my data is regularly backed up in accordance with relevant school 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

PTO

- I will not try to use any programmes or software that might allow me to bypass the filtering and security systems in place to prevent access to such materials
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this has been authorised.
- I will not disable or cause any intentional damage to school equipment or equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, when authorised to do so by a member of the Senior Leadership Team. I understand that, where personal data is transferred outside of the secure school network, it must be encrypted or password protected.
- I will not take or access pupil data, or other sensitive school data, off-site without the specific approval of a member of the Senior Leadership Team. If approved to do so, I will take every precaution to ensure the security of the data.
- I will not store any personal data belonging to pupils, their Parent Carers or other members of staff on any personal devices.
- 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 school 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 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 school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / Volunteer Name:	
Signed:	
Date:	

Acceptable Use Policy Agreement

Visitor/Community User

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

I will be responsible in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files or data, 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.

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

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful software.
- 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 and security systems in place to prevent access to such materials described above.
- 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, except with the specific approval of the school.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Visitor/Community User Name:	
Signed:	
Date:	