Woodmancote School
Belong · Aspire · Achieve

Woodmancote School and Little Chestnuts
Acceptable Use Policy

Designated Member of Staff	**School Business Manager**
Committee with responsibility	**Safeguarding**
Date of Issue	**October 2017**
Frequency of Review	**Annual**

Issue Number	Issue Date	Summary of Changes
1	October 2017	New Policy
2	March 2018	Use of encrypted memory sticks added. Section 13 and appendix 6.
3	February 2020	Reviewed by SB Added LC and use of staff mobiles on trips
4	April 2021	Reviewed
5	December 2021	Reviewed-no changes
6	October 2022	E-Safety renamed Online Safety
7	August 2023	Updated Acceptable User agreements, processes for logging concerns, Facebook guidance for staff and roles and responsibilities.
8	September 2024	Target Tracker replaced by INSIGHT

Woodmancote School
Belong · Aspire · Achieve

Contents

1 Introduction

Information Technology (IT) in its many forms (e.g. the internet, email, laptops, tablets and digital recording devices) are an important aspect of our daily lives. Consequently, Woodmancote School and Little Chestnuts aim to embrace the use of these technologies in order to help develop the skills our children will need to access life-long learning and employment. We aim to make all users (i.e. staff and pupils) of the technology (both fixed and mobile) that school provides aware of the risks so it can be used safely.

See appendix 7 for current legislation.

Disclaimer: *Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, endeavour to add any important issues to the policy on our website.*

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Woodmancote School and Little Chestnuts networked resources, including the internet, email, SIMs, Insight and Class Dojo, are intended for educational purposes, and may only be used for legal activities consistent with our school rules. Any use of the network that is either illegal or would bring the name of the school or County Council into disrepute is not allowed. As such, this policy sets out the conditions that all users are required to follow. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and/or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, whiteboards, digital video equipment, etc.)

2 CONDITIONS OF USE

Pupils

Where the user is a child, or young person, the behaviour while using the technology will be the responsibility of the supervising adult. However, children will be expected to use the technology appropriately and safely (see also guidance contained in the Online Safety policy). This will be demonstrated by pupils, in discussion with their parents or guardians (and reinforced by staff), by signing the Conditions of Use for Pupils (see Appendix 1).

At ***Woodmancote School and Little Chestnuts*** we understand the responsibility to educate our pupils on Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Staff (& or Governors, parents or visitors)

Where the user is an adult, they will be expected to use the technology for the purposes for which they have been made available. It is the responsibility of the User to take all reasonable steps to comply with the conditions set out in this policy. This will be demonstrated by agreeing to, and signing the 'Conditions of Use' (see Appendix 2).

3 Roles and Responsibilities

Governors, Head and Senior Leaders

As Online Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

Senior Leaders, Staff and Governors are updated by the Head/SBM and all have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice. This policy is also linked to the following mandatory school policies: on-line safety, safeguarding and child protection, health and safety, relationships and behaviour (including the anti-bullying), data protection policies and PSHE.

The SBM will periodically review that the Conditions of Use agreements (Appendix 1 & 2) are signed by all current users and that new staff receive information on the school's acceptable use policy as part of their induction.

All Users

It is the responsibility of all Users to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will also accept personal responsibility

for reporting any misuse of the network to the Headteacher or SBM. All staff are encouraged to incorporate Online Safety activities and awareness within their curriculum areas.

Managing Online Safety messages

We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used. The Online Safety policy will be introduced to the pupils at the start of each school year. Online Safety posters will be prominently displayed. Parents will be informed of any Online Safety updates and provided with up to date websites for information e.g. CEOP.

4 Curriculum

- The school provides opportunities within a range of curriculum areas to teach about Online Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the Online Safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.
- Pupils will be taught how to identify illegal or inappropriate content and know how to report it. Similarly, staff will have training so they know how to identify the risks and how to report them.

5 Managing infrastructure & internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. School internet access is controlled through regularly updated filtering tools. This ensures unsafe, illegal or inappropriate content is filtered. All use is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- In certain circumstances, and only for valid educational reasons that do not compromise school rules or the ethos of this policy, access to sites or software that requires the filter levels to be lifted can be granted. This will only occur where the Conditions of Use for adults (Appendix 2) has been understood and signed.
- In no circumstances will this be granted to pupils or young people.
- The school maintains students will have supervised access to internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Staff will ensure children are safe from terrorist and extremist material when accessing the internet.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

- The school does not allow pupils access to internet logs, social media and instant messaging.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the SBM using the filtering concerns form (appendix 8). Any safeguarding concerns should be raised on CPOMS.
- It is the responsibility of the school to ensure that Anti-virus protection is installed on all school machines. This automatically updates.
- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems.
- If there are any issues related to viruses or anti-virus software, the SBM should be informed.
- Woodmancote School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

6 Managing passwords & data

- All users will be provided with an individual login username. Staff will also be given a password to access the school internal server.
- All users need to create secure passwords.
- Passwords to networked resources shared by groups of users, e.g. INSIGHT, will be changed periodically, at least annually, to ensure security is not compromised.
- If any user suspects their password has been compromised, they should report it as soon as possible to the SBM to take steps to reset it.
- Any confidential data, or personal details will be stored in a password protected device or storage system (refer to Data Protection Policy).
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online Safety Policy.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.
- Due consideration should be given to security when logging into the Learning Platform to the browser/cache options (shared or private computer)

Data Security

The accessing of school data is something that the school takes very seriously.

Staff are aware of their responsibility when accessing school data. They must not;

- access data outside of school
- take copies of the data
- allow others to view the data
- edit the data unless specifically requested to do so by the Headteacher and/ or Governing Body.

7 Managing emails

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or internationally.

- Woodmancote School and little Chestnuts are aware of their responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- We use Office365 to provide all staff with an email account to be used for all school business to reduce the risk of unsolicited or malicious emails.
- Staff should not use their own personal emails to make contact with parents, pupils or other professional bodies.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- It is the responsibility of the account holder to keep their passwords and content secure.
- The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school or the LA'. The responsibility for adding this disclaimer lies with the account holder. An example is attached as an appendix to this policy (see Appendix 3). All new staff to be made aware.
- Emails sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the SBM if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Scheme of Work.

8 Managing digital recording devices

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- Woodmancote School and Little Chestnuts recognise the value of taking, publishing and storing images and sound recordings to support teaching and learning, however it also recognises that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Permission to use images of all staff who work at the school is sought on induction and a copy is located in the personnel file.
- Permission to use images of pupils, or their work, is sought on a child's entry to Woodmancote or Little Chestnuts by signing the relevant section on the Admissions form. This consent is considered valid for the entire period that the child attends this school/pre-school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/guardians may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

- Records of these permissions are kept on the school management information system (SIMs).
- Images and recordings are permitted to be used in the following ways:
  - on the school web site
  - in the school prospectus and other printed publications that the school may produce for promotional purposes
  - recorded/ transmitted on a video or webcam
  - in display material that may be used in the school's communal areas
  - in display material for use in external areas, i.e. exhibition promoting the school
  - general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Storage of Images

- Images/ videos of children are stored on the main server.
- Pupils and staff are not permitted to share images outside of school.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

9 Managing mobile devices

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

9.1 Personal Mobile devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a pupil or parent/ carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- No images or sound recordings of any pupils or young people are permitted to be stored on these devices.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

9.2 School provided Mobile devices (including phones)

- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.
- Where the school provides mobile technologies such as laptops or tablets for a pupil's personal educational use an agreement needs to drawn up about its terms of use and the responsibility of its care and maintenance between Woodmancote School and the parents or guardians.
- For offsite visits staff are permitted to use their own phone for emergencies and contact with school.

10 Facebook

The use of Facebook is not permitted on school devices. Staff should follow the guidance in appendix 4 if using Facebook on a personal basis.

11 Reporting Incidents

- Complaints about the misuse of any hardware or network resources provided by the school should be made to the Headteacher or SBM. Incidents concerning pupils should be logged on CPOMS, those concerning filtering issues should be raised by using the filtering concerns form (Appendix 8), and anything else through discussion with the Headteacher, and appropriate action taken. See Flowcharts for Managing an Online Safety Incident (Appendix 5).
- Where deliberate access to inappropriate materials by any user leads to criminal activity or is of a child protection nature, the incident could be reported, to the police. Immediate suspension or possibly dismissal could follow.
- Users are made aware of sanctions relating to the misuse or misconduct on the Acceptable Use Agreement

This policy should also be read with reference to the following supporting policies:

- Safeguarding
- Data Protection
- Online Safety

12 Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' Online Safety rules.

However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues.

Where a pupil has difficulties understanding social situations careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people.

13 Parental Involvement

- Parents/ carers and pupils are actively encouraged to contribute to the school Online Safety policy by letter and by reporting unsuitable sites etc to the School.
- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)
- The school disseminates information to parents relating to Online Safety where appropriate in the form of;
  - Website postings
  - Newsletter items

14 Use of USB Memory Sticks

Staff, Students, Visitors and Governors must not use any memory sticks, other than encrypted ones provided by the school office, to store any school information. Where appropriate, staff will be provided with an encrypted memory stick. This must be signed for, along with the memory stick agreement (see appendix 6). All memory sticks must be cleared and returned to the school office at the end of employment at the school.

Students may request a memory stick for the duration of their placement. These must be signed for, along with the memory stick agreement. They must be cleared and returned to the school office at the end of the placement.

15 Reviewing this Policy

Review Procedure
There will be an on-going opportunity in staff meetings for staff to discuss any issue of Online Safety that concerns them.

This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

Signed…… (Chair of Safeguarding)

Woodmancote School
Belong · Aspire · Achieve

Appendix 1 Acceptable Use Agreement/Online Safety Rules for Pupils

Pupils that do not follow these rules may find:

- They can only use the computers if they are more closely watched.
- They are not allowed to use the computers
- They are excluded from school

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	

Woodmancote School
Belong · Aspire · Achieve

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (parent/carer):	**Date:**

Woodmancote School
Belong · Aspire · Achieve

Appendix 1 continued

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

Woodmancote School
Belong · Aspire · Achieve

Appendix 2 Woodmancote School and Little Chestnuts Acceptable Use Agreement for Staff, Governors and Visitors

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS AND VOLUNTEERS	
Name of staff member/governor/volunteer:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer):	**Date:**

Appendix 3

Example of a disclaimer to be added to email messages sent on behalf of school business

Woodmancote School
Station Road
Woodmancote
Cheltenham
Gloucestershire
GL52 9HN

T – 01242 674312
W – www.woodmancote.gloucs.sch.uk

Woodmancote School
Belong · Aspire · Achieve

Appendix 4: Staff Facebook Guidance

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Woodmancote School
Belong · Aspire · Achieve

Appendix 5

Flow chart for Managing an Online Safety Incident

Following an incident, the Headteacher/DSL will need to decide quickly how it should be dealt with.

Unsuitable material/illegal material/unsuitable activity/illegal activity is found or suspected on school's network of resources

↓

Identify those involved, if known, without compromising any potential evidence (staff, child, visitor or unknown, and decide whether they are a victim or instigator)

↓

Isolate any equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out

↓

Report to Designated Safeguarding Lead (DSL) and/or if appropriate to the SBM

↓

Is there a child protection concern?

Yes ↓

No →

Is it an adult safeguarding concern?

Yes ↓

No →

Seek advice or make a request for Service through the Children's Helpdesk (Tel: 01452 426565)
Or Report as appropriate toLADO (Tel: 01452 426994)

↓

Is illegal or unsuitable material or activity found or suspected?

Yes ↓

Examples of illegal activity:
Downloading pornography
Passing onto others images or videos containing child pornography
Inciting racial or religious hatred
Promoting illegal acts

Allow Police or relevant organisation to complete their investigations, seeking LADO advice on treatment of victim/instigator and possible referral to DBS

↓

Is illegal or unsuitable material or activity confirmed?

Yes ↓

No →

Review incident, agree and implement appropriate actions. Suggested possible actions include:

- Inform parents/guardians
- Review or create risk assessment
- Counselling
- Referral to other agency
- Disciplinary procedures

↓

Debrief all relevant parties at end of Online Safety incident

↓

Review all policies and procedures

If you believe a child is at risk or in immediate danger you should do one of the following:

- Follow schools Safeguarding reporting procedures
- Call the Police on 999
- Or make a referral to the Social Care desk
- Immediately isolate the equipment to avoid tampering with potential evidence

Woodmancote School
Belong · Aspire · Achieve

Police or relevant organisation take action	Organise knowledge share session

Appendix 6

Woodmancote School and Little Chestnuts Use of USB Memory Stick Agreement for Staff

- When a memory stick is needed to store school information on, I will only use the encrypted memory stick provided by the school.
- I will ensure that any memory sticks previously used are wiped or returned to the school office.
- I will ensure that the encrypted memory stick is only used when it essential to store information on something other than a school computer or laptop.
- I will ensure that the memory stick allocated to me is not given to anybody else at any time.
- I will not give anybody else the password for the memory stick allocated to me.
- I will ensure that the memory stick allocated to me is kept in a safe place at all times.
- If I lose the memory stick I will inform the school office immediately.
- I will sign for the memory stick allocated to me.
- In the event that my employment / placement at the school ends I will return the cleared memory stick to the school office on my last day.

User Signature

I agree to follow this code of conduct and to support the safe use of memory sticks throughout the school and when off-site

Signature ……Date ……

Full Name ……(printed)

Woodmancote School
Belong · Aspire · Achieve

Appendix 7

Current Legislation

Acts relating to monitoring of staff email

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts relating to Online Safety

Racial and Religious Hatred Act 2006

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

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.
For more information
www.teachernet.gov.uk

Communications Act 2003 (section 127)
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)
Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

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

Woodmancote School
Belong · Aspire · Achieve

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Appendix 8

FILTERING CONCERNS FORM	
Please complete this form and email to sbm@woodmancote.gloucs.sch.uk	
Staff Name:	
Concerns Raised:	
Signed:	**Date:**

Woodmancote School

Belong · Aspire · Achieve

Woodmancote School
Belong · Aspire · Achieve

Safeguarding and child protection is at the core of all that we do at Woodmancote and Little Chestnuts and therefore relates to all policies. There are particularly important links between this child protection policy and the following policies:

Safeguarding Policies	Policies currently allocated to Premises-December 2017 which have a Safeguarding element
Acceptable Use	Accessibility Policy, Audit and Plan
Allegations against Staff	Anaphylaxis Awareness and Monitoring
Anti-Bullying	Disability Discrimination Policy and Plan
Attendance	Business Continuity Plan
Children in Care	Emergency Asthma Inhaler Policy
Code of Conduct	Fire Risk Policy and Risk Assessments
Complaints	Health and Safety Policy
Cyber Security	Lone Working Policy
Educational Visits	Lettings Policy
Equality	Security Policy
Flexi-Schooling policy	Records Management Policy
Governor's Behaviour Statement	
Intimate Care	
Lockdown	
Online Safety	
Preventing Radicalisation	
Recruitment and Selection	
Recruitment of Ex-Offenders	
Relationship and Behaviour	
Restrictive Physical Intervention	
Safeguarding and Child Protection	
SEN	
Supporting children with medical needs	
Volunteers in School	