



E-Safety Policy

This policy also applies to the EYFS

Related documents

Safeguarding and Child Protection Policy and Procedures
Spiritual, Moral, Social and Cultural Development Policy
Parent Photographic Consent Form
Anti-Bullying Policy
Withdrawal of Use of Pupil Images Form (Data Protection Policy Appendix 2)

Updated	Reviewed By	Review Date	Version
October 2025	R Gaynor	October 2026	2025.01

Contents

1	Introduction.....	3
1.1	Aims.....	3
1.2	Objectives	3
1.3	Organisation	3
1.3.1	The School:.....	3
1.3.2	Pupils are:.....	4
2	Information System Security	4
3	Unsuitable Material	5
4	Online Safety	5
5	Unacceptable Activity on Maltman’s Green Computers or Internet Access.....	7
5.1	Illegal or inappropriate activity.....	7
5.2	Additional Inappropriate Activity	8
6	Use of Mobile Technologies (tablets, e-readers and other electronic devices with imaging and sharing capabilities)	8
6.1	Staff use of mobile devices	8
6.2	Children’s use of personal mobile and electronic devices	9
6.3	Children’s use of school mobile and electronic devices.....	9
7	Email and Online Communication.....	9
8	Use of Digital Video, Images and Equipment.....	10
9	Published Content, the School Website and Social Media	10
10	Authorising Internet Access	11
11	Risk	11
11.1	Handling E-Safety complaints	11
12	Policy Review	11
13	Appendix 1: E-Learning Code of Conduct Early Years Foundation Stage (Little Malties, Nursery and Reception) and Pre-Prep (Years 1 and 2)	12
14	Appendix 2: E-Learning Code of Conduct – Prep	13
15	Appendix 3: Guidelines on Inappropriate (DELIBERATE) Internet Access	14
16	Appendix 4: Guidelines on Inappropriate (ACCIDENTAL) Internet Access.....	15
17	Appendix 5: Staff Acceptable User Policy	16
18	Appendix 6: Acceptable Use Agreement for Community Users.....	18
19	Appendix 7: Safe Use of Electronic Devices Agreement for all pupils	20
20	Appendix 8: E-Safety Procedure.....	22

1 Introduction

This policy applies to all members of Maltman's Green school community (including staff, pupils, volunteers, parents / carers, visitors and governors) who have access to the school IT systems, both in and outside school.

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 school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and confiscation of electronic devices and the deletion of data.

This policy should be read in conjunction with the School's Safeguarding and Child Protection Policy and Procedures and is written with regard to the following documents:

- Keeping Children Safe in Education, 2025
- Using Technology in Education, 2019 (updated June 2025)
- Meeting Digital and Technology Standards in schools and colleges, 2022 (updated March 2025)
- Generative Artificial Intelligence in Education (2025)

1.1 Aims

- All members of the School community, children, teachers, parents and governors, are aware of the need for safe and responsible internet use.
- The issues surrounding internet safety are discussed and clarified.
- Internet use supports the School's educational aims.
- Local education authority safeguarding requirements are fulfilled.

1.2 Objectives

- To raise awareness with pupils, staff and parents of the E-Safety issues concerning information systems, the Internet and electronic communications as a whole.
- To set out criteria for the acceptable use of information systems, the Internet and electronic communications by pupils and staff in the school.
- To identify roles and responsibilities for those staff responsible for fostering good E-Safety practice in the school.
- To identify and respond to the risks posed by providing pupils with Internet access as part of their learning experience.

1.3 Organisation

We have a whole school approach to online safety, where we aim to protect and educate pupils and staff in their use of technology. To achieve this:

1.3.1 The School:

- Has established criteria for acceptable use for Early Years Foundation Stage, Pre-Prep and Prep (see Appendices 1 and 2).
- Has designed Internet access expressly for pupil use with age-appropriate filtering.
- Has a procedure for reporting of E-Safety breaches (See Appendices 3 and 4).

- Has an acceptable use agreement for staff and volunteers (See Appendices 5 and 6).
- Has an acceptable use agreement for pupils (See Appendix 7).
- Has an E-Safety Log which is checked by the Deputy Head Pastoral at least on a monthly basis and shared at half-termly IT meetings and termly Curriculum Committee Meetings with various Governors.
- Has staff that recognise pupils may encounter E-Safety safeguarding incidents that happen outside of School and can occur between children outside of this environment. We will respond to such concerns, reporting to the appropriate agencies in order to support and protect the pupil. All staff and especially the DSL team, will consider the context of incidents that occur outside of School to establish if situations outside of their families may be putting the pupil's welfare and safety at risk of abuse or exploitation. Children who may be alleged perpetrators of E-Safety related abuse will also be supported to understand the impact of contextual issues on their safety and welfare. In such cases the individual needs and vulnerabilities of each child will be considered. Further guidance can be found at: <https://contextualsafeguarding.org.uk/>

1.3.2 Pupils are:

- Taught about acceptable use of online technologies such as the Internet, Social Media and Cloud services through a structured education programme. This teaching on E-Safety enables pupils to be aware of the dangers of and good practices associated with using all forms of technology, such as keeping their personal information private and the SMART rules for Internet use which can be found in Prep Pupils' Homework Diaries.
- Educated in effective understanding of age-appropriate research skills, including the skills of knowledge location, retrieval, evaluation and upholding copyright regulations.
- Taught to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Taught about using the Internet for research, cross-checking information before accepting its accuracy, and are shown how to share and to present information to a wider audience using various applications and platforms.
- Made aware of the impact of cyberbullying and know how to seek help if they are affected.
- Taught the importance of their 'digital footprint'.
- Taught to understand the importance of adopting good E-Safety practice when using digital technologies outside of school. They will realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the School.

2 Information System Security

System security is maintained and reviewed by the Network Manager from RM Education Ltd, who oversees the use of the School's firewalls, monitoring and filtering devices. Virus protection and anti-spam programs are updated with a regularity which is sufficient for school devices. Security strategies are discussed and actioned with the IT Strategy group and at scheduled SLT meetings. The monitoring and filtering system is managed and reviewed by the Network Manager, Head of Digital Learning, Deputy Head Pastoral and the Headmistress.

The school uses RM SafetyNet as our web filtering product, which is used by thousands of schools across the UK and is recommended for use on the Digital Marketplace section of the Gov.uk website. RM Education is also a member of the IWF (Internet Watch Foundation) and has been since 2004 as well as an accredited member of the UK Safer Internet Centre, Childnet and the South West Grid for learning (SWGfL). In order to be a member of the SWGfL RM must undertake regular safety and security checks on their web filters. Membership of the SWGfL also confirms that our filtering provider is signed up to relevant lists (including CSA content, Sexual Content, Terrorist content and Your Internet Connection Blocks Child Abuse & Terrorist Content).

All staff have annual training in Cyber Security and are aware of their responsibilities and the need to report anything suspicious immediately to our Network Manager and the DSL, who will then alert the Headmistress.

We share information about the systems we use to filter and monitor online use with parents at the beginning of each academic year, along with other E Safety information (please see section 4 for further details). We write to parents with details of any new sites we are introducing for use at home and/or school. Parents are also able to view which sites their daughter's have access to via their daughter's RM Unify account. Details for programmes that are not linked to RM Unify, such as our Online Library Platform, are detailed in the front of each pupil's school planner.

3 Unsuitable Material

Should any unsuitable online material be found by staff, pupils or other users of the School network, they must be reported to the Designated Safeguarding Lead and Network Manager. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, the correct procedures must be used to investigate, preserve evidence and protect those carrying out the investigation. The school will deal with incidents that involve accessing inappropriate websites through the use of an internal filtering system which actively blocks known sites which harbour inappropriate content.

4 Online Safety

As the School increasingly works online, it is essential that children are safeguarded from potentially harmful and inappropriate material. The school invests in a key-stroke monitoring system, Smoothwall, which sends immediate alerts of any concerning activity to the DSL and DDSLs. The DSL also receives a weekly activity report from Smoothwall.

Any concerns are thoroughly investigated and reported to parents if necessary. E-Safety Logs detailing these concerns are kept by the DSL and DDSL Team and are reviewed at least on a monthly basis with the wider Team, the Headmistress and the Designated Safeguarding Governor. In addition to this, the school maintains a variety of filtering systems to ensure that children can only access appropriate content. E-Safety also forms an agenda item at half-termly ICT meetings, termly Curriculum Sub Committee meetings with relevant governors (including the nominated Safeguarding Governor) and during the DSL's weekly meeting with the Headmistress.

If any issues arise through our Logs or our monitoring and filtering systems that we feel parents should be aware of, then we circulate information to our parent body. For example, as

it becomes apparent that children are accessing a platform at home which they are not old enough to use, we alert our parent body to this and provide information and support.

The School does not permit pupils to have access to mobile phones in and around our School site. For further details about how our mobile phone procedures and how we limit the possibility of a child accessing the Internet using 3G, 4G and 5G, please see relevant sections of our Safeguarding and Child Protection Policy and Procedures.

Staff receive regular training on E-Safety, which takes place at Induction and during termly Safeguarding updates at the start of each term on the INSET days. In addition to this, staff guidance and resources to teach children are shared throughout the year by our Head of Digital Learning.

At the start of every academic year, our E-Learning Codes of Conduct for different phases of the school are shared with the children and their parents. Parents/children (age appropriate) sign to say that they have read and understood these documents. These documents can be viewed in appendix 1 and 7 of this Policy. Staff also sign an annual Staff Acceptable User Agreement. Parental permission is also sought for the use of webcams should there ever be a need for periods of Distance Learning from home. Guidance for parents on how to help keep their children safe online is also shared with parents at the same time. Please see appendix 8 for further information. Buckinghamshire County Council also provide information for professionals relating to E-Safety. This can be viewed via the following link: [Bhttps://www.buckssafeguarding.org.uk/childrenpartnership/professionals/E-Safetyadvice-and-information/](https://www.buckssafeguarding.org.uk/childrenpartnership/professionals/E-Safetyadvice-and-information/)

Online safety is also explicitly taught in Computing lessons at the beginning of the year, and periodically as part of the overall curriculum.

This E-Safety policy provides further details of the ways in which we can support and teach children about this aspect of modern life. The School also takes part in the Safer Internet Day, making it into an E-Safety Week annually in February. Additional information on E-Safety is also provided in Part 2, Part 5, Annex B and Annex C of Keeping Children Safe In Education 2025 and in the following guidance:

- [DfE advice for schools: teaching online safety in schools](#)
- [UK Council for Internet Safety \(UKCIS\) guidance: Education for a connected world](#)
- [UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [The UKCIS external visitors guidance](#) will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors
- [National Crime Agency's CEOP education programme: Thinkuknow](#)
- [Public Health England: Every Mind Matters](#)
- [Harmful online challenges and online hoaxes](#)— this includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.

Where appropriate for primary school aged children, pupils, staff and parents/carers are supported to understand the risks posed by categorising them into four areas of risk:

1. the **CONTENT** accessed by pupils. They could be exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
2. their **CONDUCT** online, recognising that their personal online behaviour could increase the likelihood of, or cause harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nude and semi-nude and/or pornography, sharing other explicit images and online bullying.)
3. who they have **CONTACT** within the digital world. They could be subjected to harmful online interaction with other users, for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
4. **COMMERCE** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If staff, parents/carers feel a child is at risk, please report it to the Anti-Phishing Working Group at apwg.org/

Cyberbullying is the act of bullying others over the internet or on a mobile phone by sending abusive emails or texts directly or by posting nasty comments or humiliating messages for others to see. Cyberbullying is a way to describe common forms of bullying, such as name calling, racism, homophobia, sexism etc., which happens online. Like any form of bullying, cyberbullying can be horrible for the children involved and hard for them to talk about. Pupils are encouraged to report any form of cyberbullying to an adult and not to ignore it.

Cyberbullying by children, via texts, social media and emails, will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

5 Unacceptable Activity on Maltman's Green Computers or Internet Access

The following is separated into two categories

5.1 Illegal or inappropriate activity

The School believes that the activities listed below are inappropriate in a school context (those in bold are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school). 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** (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** (illegal–Criminal Justice and Immigration Act 2008);
- **criminally racist material in UK criminally racist material in UK–to stir up religious hatred (or hatred on the grounds of sexual on the grounds of sexual orientation)** (illegal– Public Order Act 1986);
- democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs (Prevent Strategy 2011 – See SMSC policy);
- pornography;
- promotion of any kind of discrimination;
- promotion of racial or religious hatred;
- threatening behaviour, including promotion of physical violence or mental harm; or

- any other information that may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

5.2 Additional Inappropriate Activity

It is important that any incidents are dealt with as soon as possible in a proportionate manner (in line with appendix 4), 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 disciplinary procedures. The following is also considered to inappropriate activity at Maltman's Green School:

- using school systems to run a private business;
- use systems, applications, websites, or other mechanisms that bypass the filtering or other safeguards employed by the school (i.e. proxy services);
- uploading, downloading, or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords);
- 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;
- online gambling and non-educational gaming;
- use of personal social networking sites and profiles for non-educational purposes.

6 Use of Mobile Technologies (tablets, e-readers and other electronic devices with imaging and sharing capabilities)

6.1 Staff use of mobile devices

The school recognises that ownership and use of mobile technology (Tablets, ereaders and other electronic devices with imaging and sharing capabilities) is increasing rapidly, and we are happy to allow the use of this technology in school. The following applies when using mobile technologies:

- Members of staff are allowed to bring their personal mobile device into school. However, they are required to use their devices only in the designated areas authorised by the SLT, or in an area where no children are present.
- All members of school staff must not use their mobile/electronic devices with imaging and sharing capabilities for personal use in the Early Years Foundation Stage.
- They must only use and take pictures of pupils on school devices and the pictures that they take must remain in school and be deleted once used.
- Some members of staff have mobile phones for work use e.g. members of the SLT and caretakers (for making and receiving work calls) and Peris will have to take registers using a paper register. They can use an iPod or a school iPad, but not their mobile phone or other electronic device with imaging and sharing capabilities. The school reserves the right to check the contents of the mobile phones or other electronic device with imaging and sharing capabilities of any staff who may have

used such items on the School site at any time. These staff are made aware of our procedures.

- As they sign in, visitors and volunteers are also requested to turn off their mobile phones or other electronic devices with imaging and sharing capabilities and to store them out of view from the children.
- We have signs around our school indicating that we are a mobile phone free site. Our staff support and fully understand. Furthermore, we strongly encourage all visitors to refrain from mobile phone or other electronic device with imaging and sharing capabilities use on site. Staff are encouraged to challenge the use of unregulated mobile phone or other electronic device with imaging and sharing capabilities use.
- In the case of an event, parents should not film or photograph their children during the event/performance, and any photos/film taken before or afterwards must not be shared on social media.

6.2 Children's use of personal mobile and electronic devices

Maltman's Green School does not allow pupils to bring electronic devices into School, this includes Smart watches (meaning that they would not be able to access 3G/4G/5G services). The exception is Year 6 children who have permission to walk to or from School. Should their parents wish them to have a mobile phone, they must hand their device in at main Reception upon their arrival at School, and collect it at the end of the school day. It is always possible that a pupil may keep their phone with them during the day without permission, therefore, staff and pupils should remain vigilant.

Pupils are not permitted to bring any mobile or electronic devices with imaging and sharing capabilities, including Smart watches or cameras on school trips, instead with parents' consent, staff members take pictures of the children using school cameras during outings/residential trips and these images are then shared with parents after the trip.

6.3 Children's use of school mobile and electronic devices

Pupils are only allowed to take pictures/film each other, for example on the School iPads, when permission is given by a member of staff when the pictures are necessary for a supervised class-based activity, such as completing a project.

7 Email and Online Communication

- Access to email is provided for all users in school via both Outlook desktop and Outlook Online. Users should be aware that email communications are secure and may be monitored. Pupils must be notified of the expectations of communication; that use of communicative resources between pupils and teachers is only when teachers have authorised it.
- Staff may only access personal email accounts on school systems and must use their own professional judgment as to when it is appropriate to use them (these may be blocked by the filtering systems). However, access is made available to these accounts via an unrestricted proxy path issued to staff. This pathway is monitored and filtered by the security systems listed in Staff Acceptable User Policy (Appendix 5 - **item 14**). In addition, staff must sign an AUP (Acceptable Use Policy) before they are granted access (see Appendix 5).
- Users must **immediately** report the receipt of any email or communication that is offensive or makes them feel uncomfortable. Users must treat incoming messages

and posts from unknown sources as suspicious and should not open attachments unless the author is known. Emails or communication of this nature must not be deleted to aid any investigation process.

8 Use of Digital Video, Images and Equipment

When using digital images staff should inform and educate pupils about the risks associated with the taking, storing, and distributing images. In particular, all pupils are barred from access to social media and social networking sites. Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

- Images should only be captured using school equipment. The use of personal equipment should not be used for such purposes.
- Care should be taken when taking digital images or video, that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Staff must refer to photographic consent list before using pictures of children in any promotion of the school. Children whose parents have not given Maltman's Green School photographic consent must not have their pictures distributed publicly. More detail on this can be found in the 'Parent Photographic Consent Form', which is shared with parents when their daughters join the school.

9 Published Content, the School Website and Social Media

Maltman's Green uses its website to inspire children with achievements that have been made during the term and to inform all stakeholders of key events and key information pertinent to the running of the School. The website reflects the School's ethos and that information contained within it is accurate and well presented.

- Editorial responsibility will lie with Headmistress and Director of Marketing. This is in order to ensure that content is accurate, and quality of presentation is monitored.
- All material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- The point of contact on the website should be the School address and telephone number. Home information or individual email identities will not be published.
- Photographs must not identify individual children. Group shots will be used in preference to individual "passport" style images.
- Full names will not be used anywhere on the website, particularly alongside photographs.
- Parents who do not wish for images of their children to be used by the School must opt out by responding to the school communication regarding photographic consent.
- Staff and children will be made aware that the quality of their work published on the web needs to reflect the standard of work expected at Maltman's Green School.
- Access to social media sites is controlled and monitored. Access is blocked to pupils, and all are educated in their safe use within lessons.

- Staff are also blocked from accessing social media via the filtered school network and are required to use their own professional judgement as to when it is appropriate to use them when on the school grounds, or on school business.

10 Authorising Internet Access

- All staff and pupils must read and sign the Acceptable Use Policy (Appendix 5) before using any ICT resource.
- Visiting speakers and guests who wish to use the WiFi or computers must agree to the terms communicated on arrival at Maltman's Green School
- If a pupil or member of the school community accidentally or deliberately accesses an inappropriate website the school guidelines must be followed (see Appendices 3, 4 and 5).

11 Risk

- All reasonable precautions are taken to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Ultimately, the school cannot accept liability for any material accessed, or any consequences of Internet access.
- Teachers discuss the risks of potential E-Safety issues associated with information systems, mobile devices, the Internet and electronic communications as a whole. Parents are also informed of these issues via the School newsletter, relevant SchoolPosts (email system) and occasionally through organised speakers.
- Emerging technologies are examined for educational benefit, and a risk assessment will be carried out before use in school is allowed. The school is aware that technologies which are not connected to the school network such as mobile devices with 3G, 4G and 5G Internet access can bypass school filtering systems and present a new route to undesirable material and communications.








11.1 Handling E-Safety complaints

In reference to complaints regarding misuse, the School's complaints procedure should be followed

12 Policy Review

This policy is reviewed on an annual basis after discussion with staff, pupils, parents and members of the Senior Leadership Team.

13 Appendix 1: E-Learning Code of Conduct Early Years Foundation Stage (Little Malties, Nursery and Reception) and Pre-Prep (Years 1 and 2)

<p>These rules help us to stay safe on the Internet:</p>	
	<p>I will ask an adult if I want to use a computer/Tablet</p>
<p>I will only use activities that an adult says are OK</p>	
	<p>I will take care of the computer /Tablet and other equipment.</p>
<p>I will ask for help if I am not sure what to do or if something has gone wrong.</p>	
	<p>If I see something I don't like on a screen, I will always tell an adult.</p>
<p>I know that if I break the rules I might not be allowed to use a computer.</p>	
<p>I will only use a computer/ tablet in a shared/family area.</p>	

14 Appendix 2: E-Learning Code of Conduct – Prep

‘BE RESPONSIBLE & STAY SAFE ONLINE’

I understand that while I am a member of Maltman’s Green 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, wherever possible be supervised and monitored.
- I will keep my password safe and will not use anyone else’s (even with their permission).
- 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 only use my own personal ICT kit if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- 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 programs on ICT devices belonging to the school unless I have permission.
- I will only use school approved platforms and programs to communicate with others. 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:

15 Appendix 3: Guidelines on Inappropriate (DELIBERATE) Internet Access

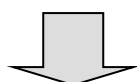
Whilst using the Internet during school hours, a pupil **deliberately** types in a website address that will display inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for dealing with pupils deliberately searching for inappropriate materials on the Internet.

Explain to the pupil that they have broken the rules of your school's Acceptable Use Agreement, and that their behaviour is unacceptable.



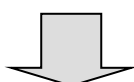
Take the pupil off the computer for the duration of the lesson. At a convenient time, ask the pupil to explain what happened and tell them that by doing so they may lessen the seriousness of the incident.



Draw the pupil's attention to the Acceptable Use Agreement that they agreed with their parents on starting at the school and which is displayed in your ICT area.



Discuss the incident with the Headmistress, Deputy Head Pastoral or Deputy Head Academic. Fill out a pastoral communication form regarding the incident, and report it to Network Manager so that the filtering can be improved accordingly.



Report the incident to the Deputy Head Pastoral. All forms should be passed to DHP. Decide the sanctions and, if appropriate, inform the pupil's parents and explain the action taken by the school

16 Appendix 4: Guidelines on Inappropriate (ACCIDENTAL) Internet Access

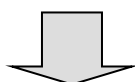
Whilst using the Internet during school hours, a pupil **accidentally** finds a website displaying inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for reporting inappropriate materials from the Internet.

Praise the pupil for reporting the incident or explain they should have reported it in line with the school's E-Learning Code of Conduct, 'Be Responsible – Stay Safe on the Internet.'



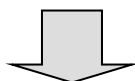
Explain to the pupil that, in order to prevent it occurring again, you need to ascertain how the pupil gained access to the inappropriate material.



Ask the pupil to explain what happened



Email RM Support with details of the incident so that filtering can be improved and notify the Headmistress and Deputy Head Pastoral Fill out a pastoral communication form regarding the incident.



**Pass on the pastoral communication form to the Deputy Head Pastoral.
If appropriate, inform the pupil's parents to explain the preventative action taken by the school.**

17 Appendix 5: Staff Acceptable User Policy



Staff Acceptable User Policy

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all adults are aware of their professional responsibilities when using any form of IT. The main priority of all adults when they are using the Maltman's Green School IT facilities should be to safeguard the children. All staff are expected to sign by accepting this agreement on first use of the school network at the start of each term. All adults are expected to adhere at all times to its contents. Any concerns or clarification should be discussed with the Headmistress.

1. I will only use the school's network, email and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headmistress or Governing Body.
2. I will create a strong password in order to protect the school network (see the Staff Handbook for more details T:\Staff Resources\AA Key Staff Resources\Key School documentation pdf\Handbooks).
3. I will never disclose or share my password. Passwords should be changed regularly (at least annually), memorised and never written down.
4. I will make no attempt to bypass system or network security settings.
5. I will ensure that all electronic communications with pupils and adults are compatible with my professional role.
6. I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
7. I will only access the school network from a secure computer or device, which is in a private and secure location and has the latest security updates, along with up to date Anti-virus software.
8. I will only use the approved, secure e-mail system for any school business.
9. I will ensure that personal data (such as data held in the school MIS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data must be treated responsibly at all times.
10. I will never attempt to install any hardware or software on to the school system. All hardware and software are installed by the Network Manager, subject to approval and appropriate licences.

11. I understand that as a member of staff I have reduced filtered access to the internet. I will use this access safely and responsibly.
12. I will only use my personal mobile phone in the areas designated by the SLT or in an area where no children are present
13. I will not browse, download, upload or distribute any material that could be considered offensive, illegal, discriminatory, or counter to British Values.
14. Data / images of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carers, member of staff or Headmistress.
15. I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community. I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headmistress.
16. I will respect copyright and intellectual property rights. Any copyright material downloaded should be appropriately identified. The use of this material is subject to the provisions of copyright law.
17. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
18. I will treat email as a means of professional communication at all times. Senders should remember that there is always a risk of misinterpretation; messages should be polite and avoid any strong language or over-familiarity.
19. I will support and promote the school's E-Safety and Data Security policies and help pupils to be safe and responsible in their use of IT and related technologies.
20. I will not allow any pupil to have access to my social networking pages and I will set my privacy settings appropriately. I will never accept a pupil as a friend, nor be a pupil's friend on any such site. I will seek to avoid personal or professional embarrassment by considering carefully the publication of personal information and pictures on such sites, or when making any online comments that may relate to the school.
21. I understand that complying with this agreement is a requirement of employment at Maltman's Green school.

18 Appendix 6: Acceptable Use Agreement for Community Users



This Acceptable Use Agreement is intended to ensure that:

1. Community Users (guests, volunteers, FOMG etc) of Maltman's Green School digital technologies will be responsible users and stay safe while using these systems and devices
2. Maltman's Green School systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and its users at risk.
3. That users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

4. I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the Maltman's Green School
5. I understand that my use of (Maltman's Green School) systems and devices and digital communications will be monitored
6. I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
7. 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 software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
8. I will immediately report any illegal, inappropriate, harmful material or incident that I become aware of, to the appropriate person.
9. I will not access, copy, remove or otherwise alter any other user's files without permission.
10. I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published, it should not be possible to identify those images by name, or other personal information.
11. I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
12. I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
13. I will not install or attempt to install programs of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

14. I will not disable or cause any damage to Maltman's Green School equipment, or the equipment belonging to others.
15. I will immediately report any damage or faults involving equipment or software, however this may have happened.
16. I will ensure that I have permission to use the original work of others in my own work
17. Where work is protected by copyright, I will not download or distribute copies (including music and videos).
18. I understand that if I fail to comply with this Acceptable Use Agreement, the Maltman's Green School has the right to remove my access to school systems / devices.

I have read and understand the above and agree to use the school ICT 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.

19 Appendix 7: Safe Use of Electronic Devices Agreement for all pupils



Safe Use of Computers Agreement

- I will only use IT in school for school purposes.
- I am only allowed to use the school computers when they are supervised by a member of staff.
- I will only use my own school email address when emailing.
- I will only open emails and email attachments from people I know, or who my teacher has approved.
- I will not tell other people my passwords.
- I will only open or delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher or parents immediately.
- I will not use an Internet-enabled device without adult supervision.
- I will not give out my own details such as my name, phone number or home address.
- I will never arrange to meet someone who I have met online.
- I will not access any social networking sites from school at any time, or at home, unless I am old enough to meet the terms of the site (this is 13 for most sites).
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I am aware of the SMART Rules and I will remember them when I am using the Internet.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.

I know that my use of IT can be checked and that my parent/carer may be contacted if a member of school staff is concerned about my safety.

20 Appendix 8: E-Safety Procedure

