Diocese of Chelmsford Vine Schools Trust

The Diocese of Chelmsford

Vine Schools Trust

E-Safety & Internet Use Policy

Revised by: A Eaves, Sep 2019

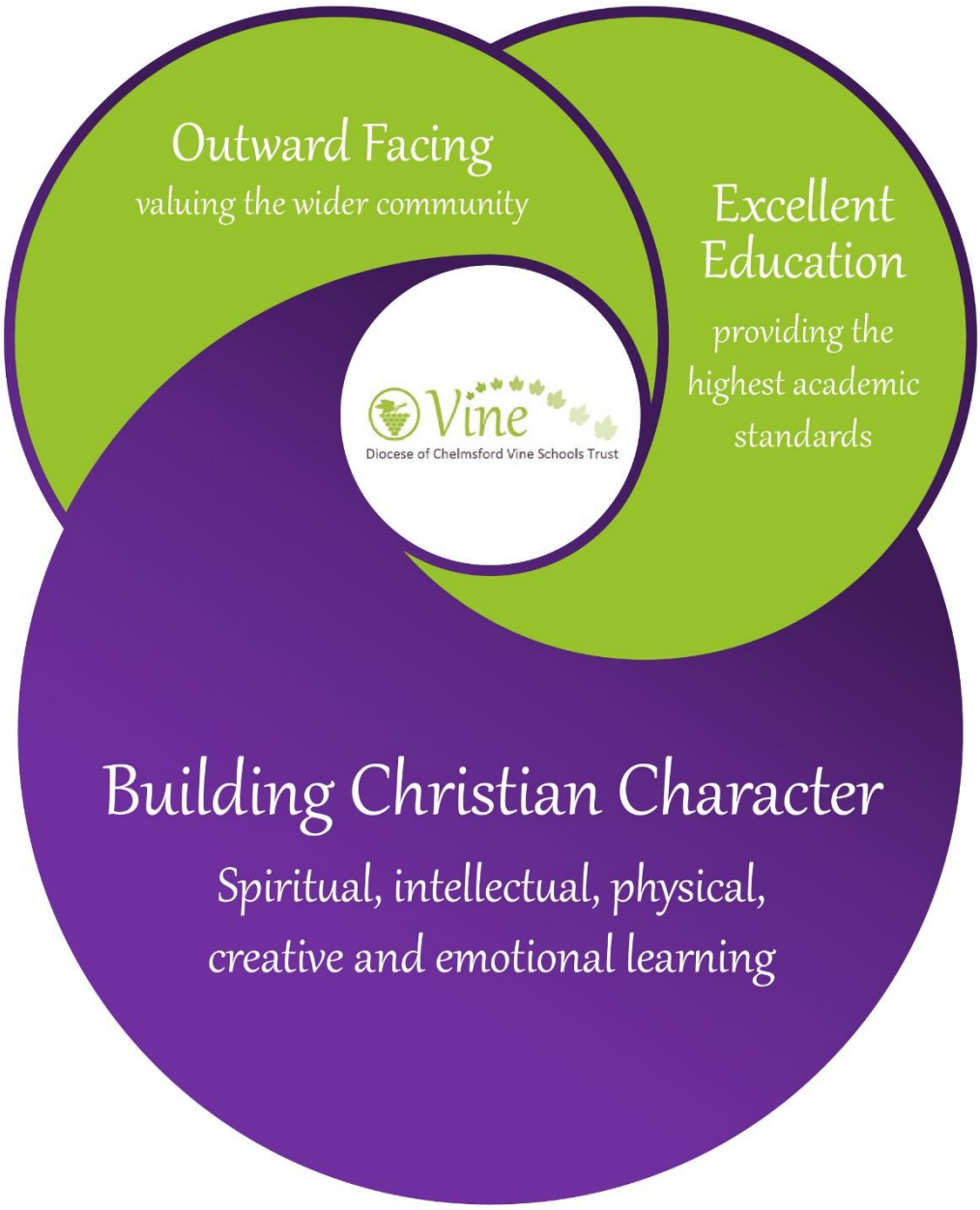
Date of Review: Sep 2020

The Diocese of Chelmsford Vine Schools Trust	
Approved by:	The Vine Schools Trust
Signature:	Chairman
Date:	

Howbridge Church of England Junior School	
Approved by:	Local Governing Body/Local Board
Signed (Chair of Local Governing Body/Local Board)	
Date:	

Policy Reference:	I002
Version No:	V2.0 – Oct 2020
Next review date:	Autumn 2021

Our Vision and Values



CONTENTS **PAGE NO:**

1. **Introduction**.....5
2. **Why Internet Use is Important**.....6
3. **Using the Internet for Learning**.....6
4. **Evaluating Internet Content**.....7
5. **Internet Use by Staff**.....7
6. **E-Mail**.....7
7. **Managing the IT infrastructure**.....6
8. **Publishing Pupils' Images and Work**..... 9
9. **Mobile Devices**.....6
10. **Electronic Communication**.....6
11. **Downloads**.....6
12. **Filtering**.....7
13. **Emerging Technologies**.....7
14. **Online Bullying (Cyberbullying)**.....7
15. **Handling Incidents**.....7
16. **Authorising Internet Access**..... 7
17. **Review**..... 8

This Policy must be read in conjunction with other policies such as the Code of Conduct Policy, Anti-Bullying Policy and CP/Safeguarding Policy.

1. Introduction

1.1 We are committed to using Information and Communication Technology and all it offers to promote learning in the most effective and appropriate way at Howbridge Church of England Junior School - for the benefit of our pupils, staff and community. To this end, we have developed this Acceptable Use Policy, to provide safeguards and ensure that all members of Howbridge community understand the benefits, risks and what is expected of them when they use ICT in the learning environment.

1.2 Our policy consists of:

- Statements outlining our Academy's approach and attitudes towards using Information & Communications Technologies safely and responsibly;
- Sets out the key principles expected of all members of the school community at Howbridge with respect to the use of IT-based technologies;
- Clear guidelines and rules for acceptable use of ICT;
- Aims to safeguard and protect children and staff;
- Ways to assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice;
- Clear structures to deal with online abuse such as on-line bullying (noting that this needs to be cross referenced with other school policies);
- There are also Internet Use Agreements, to be signed by parents, staff and pupils;
- Guidance so that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

1.3 Howbridge's computing subject leader, Mr A Eaves, will also act as the e-safety coordinator supported by the Designated Safeguarding Lead and the Headteacher, Mrs L Dale. The e-Safety Policy and its implementation will be reviewed regularly to ensure that it remains fit for purpose.

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

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Details of the Roles and Key Responsibilities of staff at Howbridge can be found in Appendix 1.

2. Why Internet Use is Important

2.1 We believe the internet is an essential element in the 21st century life for education, business and social interaction.

2.2 Howbridge recognises its duty to provide children with quality Internet access as part of their learning experience.

2.3 Using the internet and ICT in general is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.4 Pupils are increasingly using the internet and a range of ICT devices outside of Academy life and therefore need to learn how to evaluate information and to take care of their own safety and security.

3. Using the Internet for Learning

3.1 We teach all of our pupils how to find appropriate information on the internet and how to ensure as far as possible, that they understand who has made this information available and how accurate and truthful it is.

3.2 Teachers carefully plan all internet-based teaching and lessons, including e-Safety sessions, to ensure that pupils are focused and using appropriate and relevant materials.

3.3 Children are taught how to use search engines and how to evaluate internet-based information as part of the computing curriculum, and in other curriculum areas where necessary.

3.4 Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use.

3.5 Staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, .e.g.. use of passwords, logging-off, use of content, research skills and copyright.

3.6 Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

3.7 Processes are in place for dealing with any unsuitable material that is found during internet use (see section on managing filtering).

3.8 Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit. Pupils who need to search individually will be in the upper primary years. Teachers, wherever possible, will have viewed the content prior to use to check its relevance and suitability.

3.9 Howbridge's internet access includes filtering appropriate to the age of our pupils which is provided by an approved supplier.

3.10 Howbridge enables the pupils to access the internet at lunchtime as part of a range of activities

for young people. There are clear guidelines as to what is accessed and it is monitored by the SLT on duty at lunchtime, regulated in access by the teaching staff and specialist ICT support staff.

3.11 We provide awareness and training sessions for parents/carers during our transition information evening.

3.12 Run sessions throughout the year either in-house or through support agencies on e-Safety.

3.13 Promote e-Safety and provide parents/carers with advice and guidance regularly on our newsletters and website.

4. Evaluating Internet Content

4.1 The Academy will ensure that staff and pupils are mindful of copyright regulations when copying, downloading and representing materials from the internet. Web-based resources have similar copyright status to printed and recorded materials, such as books, films and music, and this must be taken into consideration when using them.

4.2 Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

4.3 Pupils will be taught how to carry out simple checks for bias and misinformation. Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

5. Internet Use by Staff

5.1 Howbridge understands that the internet is a valuable resource for Academy staff. It provides a wealth of resources, teaching materials and information that we can use to support and enhance learning. It allows staff to share resources with other academies, and to engage in debate and discussion on educational topics and news.

5.2 It also provides an efficient way to access information from the Department for Education and other government agencies and departments that will help staff to keep abreast of national and local developments.

5.3 There are also increasing opportunities for staff to access INSET and Continuing Professional Development activities using the Internet and e-learning resources.

5.4 We are committed to encouraging and supporting our staff to make the best use of ICT and all the opportunities it offers to enhance our teaching and support learning.

5.5 We provide regular training to staff on on-line safety issues and the school's on-line safety education programme.

5.6 Staff use of the internet on Howbridge computers will be responsible and legal at all times and in keeping with their professional role and responsibility. Misuse of the internet and Howbridge computer systems will be rigorously investigated.

5.7 As part of the induction process, all new staff (including those on university/college placement and work experience) provided with information and guidance on our policies and the school's Acceptable User Agreement.

5.8 Further guidance can be found in the Code of Conduct Policy.

6. E-Mail

6.1 E-mail is one of the many modes of communication which plays an important role in many aspects of our lives today. We teach the use of e-mail as part of our computing curriculum by means of Google mail. Open email contact is not possible and an objectionable language filter is in place. This provides a limited facility and yet it gives all the structure of using actual email.

6.2 In spite of this not being an open facility the opportunity is taken to educate children to be aware of the benefits and risks and how to be safe and responsible users as part of our e-safety provision.

6.3 Pupils are taught strategies to deal with inappropriate emails and are reminded of the need to write emails clearly and correctly, not including any unsuitable or abusive material.

6.4 Pupils are taught not to reveal personal details of themselves or others in e-mail communication, nor to arrange to meet anyone without specific permission.

6.5 Staff are encouraged to use the Academy email service and accounts that are available. They are more secure and are easier to access by a third party should the need for scrutiny arise. Personal web based email accounts are also permitted but discouraged for professional communications.

6.6 Staff should always ensure that they represent the Academy in a professional and appropriate way when sending e-mail, contributing to online discussions or posting to public websites. Failure to do so could lead to disciplinary action being taken

6.7 We provide staff with an email account for their professional use and makes clear personal email should be through a separate account;

6.8 We use anonymous or group e-mail addresses, for example office@howbridge-jun.essex.sch.uk.

6.8.1 We will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law.

6.8.2 We use a number of technologies to help protect users and systems in the school, including desktop anti-virus product McAfee, plus direct email filtering for viruses.

6.9 Staff should avoid using email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

6.7 Further guidance can be found in the Code of Conduct Policy.

7. Managing the IT infrastructure

7.1 Internet/email access is monitored and staff are reminded to use any of Howbridge IT equipment in a professional capacity

7.2 Howbridge uses the Essex filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status

7.3 The network health is protected through use of McAfee anti-virus software via ZenZero

7.4 Howbridge uses individual, audited log-ins for all users;

7.5 Guest accounts are occasionally provided for external or short term visitors for temporary access to appropriate services;

7.6 We ensures the Systems Administrator/network manager is up-to-date with relevant services and policies

7.7 Daily back-up of school data (admin and curriculum) as secure 'Cloud' storage is undertaken through ZenZero and conforms to DfE guidance;

7.8 Storage of all data within the school will conform to the EU and UK data protection requirements – see GDPR Policy

7.9 To ensure the network is used safely, this school:

7.9.1 Ensures staff read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. The same credentials are used to access the school's network;

7.9.2 All pupils have their own unique username and password which gives them access to the Internet and other services;

7.9.3 Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;

7.9.4 Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

7.9.5 Requires all users to log off or have a screen lock down when they have finished working or are leaving the computer unattended;

7.9.6 Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school approved systems:

7.9.7 This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;

7.9.8 Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX)

7.9.9 Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;

7.9.10 All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

7.9.11 Stickers are placed over webcams to limit the chance of hackers gaining access to images inside school.

7.10 Password policy

7.10.1 Howbridge makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.

7.10.2 All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.

7.10.3 We require staff to use STRONG passwords.

7.10.4 We encourage staff to change their passwords regularly.

7.10.5 We require staff using critical systems to use two factor authentications.

8. Publishing Pupils' Images and Work

8.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images and video that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images / video on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

8.2 Pupils are taught about how images can be manipulated in their on-line safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work

8.3 Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

8.3 Howbridge will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

8.4 Staff are allowed to take digital / video images to support educational aims, but must follow the Howbridge policy concerning the sharing, distribution and publication of those images which states that:

8.4.1 Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute or danger;

8.4.2 Nobody should take, use, share, publish or distribute images of others without their permission;

8.4.3 Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images;

8.4.4 Pupils' full names will not be used anywhere on the website or learning platform, particularly in association with photographs;

8.4.5 We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement for when their daughter/son joins the school;

8.4.6 Parents or carers are informed of our policy on publishing and are able to opt their children out.

8.4.7 If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental permission for its long term, high profile use;

9. Communication Technologies

9.1 Most of these modes of electronic communication are restricted at Howbridge however they are being used more frequently by pupils and staff outside of the Academy.

9.2 We acknowledge social networking sites, blogs, instant messenger services, chat rooms and forums are beneficial for communication, learning and research. They also present a range of personal safety and privacy issues.

9.3 In Academy time, pupils and staff are not permitted to access social networking sites, public chat rooms, discussion groups and forums etc. using Academy resources. Most are blocked by the filtering service used by the Academy.

9.4 Social networking:

9.4.1 Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications. We teach a unit on blogging and social networking in Upper school all of which is monitored by staff.

- For the use of any school approved social networking staff, will adhere to school's user agreement. Updates onto our Twitter/Facebook is only allowed by agreed personnel.

9.4.2 School staff will ensure that in private use

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any current pupil. Any exceptions must be approved by the Headteacher. Staff are advised to protect themselves by exercising caution and carefully consider whether to have ex pupils/parents/carers as 'friends' on social networking sites;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

9.4.3 Pupils

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Pupils are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement

9.4.4 Parents

- Parents are reminded about social networking risks and protocols through our parental communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

10. Mobile Devices (phones, tablets etc)

10.1 We anticipate that more and more of our pupils will have access to internet-enabled devices such as mobile phones or other hand held devices which are capable of browsing and uploading to the internet, accessing email and social networking services, as well as taking photos and recording video.

10.2 Howbridge recognises the potential advantages these devices can offer for staff and pupils and there are clear and enforceable rules for their use.

10.3 Pupils are taught the legal and moral implications of posting photos and personal information from mobile phones to public websites and how to use these technologies in a safe and responsible manner.

10.4 Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

10.5 Pupils are encouraged not to bring in their own mobile devices; permission should be sought from the Headteacher before any such item is brought in. The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. If pupils bring in their phone they are kept in a secure place by the class teacher until the end of the school day.

10.6 Staff should represent Howbridge in a professional and appropriate way when communicating via the internet, contributing to online discussions or posting to public websites using Academy facilities.

10.7 Teachers are issued with an iPad and laptop for professional use. The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device. PIN access to the device must always be known by the network manager.

10.8 Personal mobile devices will not be used during lessons or formal school time unless as part of an

approved and directed curriculum-based activity with consent from Headteacher / SLT.

10.9 Personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the child leaves the premises at the end of the day.

10.10 Staff members may use their phones during school break times, in the agreed place e.g.. the staffroom. In emergency situations staff may have their phones switched on if they need to take an urgent call; permission needs to be sought from the Headteacher or Assistant Headteacher prior to this.

10.11 Staff are allowed to use their own mobile phone whilst off site with pupils to enable them to contact the school, parents or carers as required.

10.12 All visitors are requested to keep their phones on silent.

10.13 The recording, taking and sharing of images, video and audio on any personal mobile device of the school or pupil is not permitted

10.14 The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material

10.15 If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

11. Electronic Communication

11.1 Communication between children and Academy staff should take place within clear and explicit professional boundaries.

11.2 Staff must be careful not to share any personal information with children such as personal email, web based communication facilities, home or mobile numbers. They should not request, or respond to, any personal information from the child / young person, other than that which might be appropriate as part of their professional role.

11.3 Staff should ensure that all communications are transparent and open to scrutiny. In addition all staff must be sure of their social networking and uphold professional confidentiality at all times. As a staff we have agreed that we should exercise caution when accepting parents as 'friends' on social contact sites such as Facebook. Staff should not accept pupils as 'friends' on social contact sites: the only exception are family members that may attend the school.

12. Downloads

12.1 The Internet is a rich source of free files, applications, software, games and other material that can be downloaded and installed on a computer. Whilst some of this material may be useful, much is inappropriate, and may adversely affect the performance and reliability of Academy equipment.

12.2 Pupils are not allowed to download any material from the internet unless directed to do so by an appropriate staff member.

12.3 Staff should take care that files from both other computers outside the Academy and internet are checked for virus contamination before they are used on the Academy system.

12.4 Pupils are not allowed to use CDs, DVDs or memory sticks brought from home or, for example, from magazines unless they have been given permission.

12.5 The Academy subscribes to suitable antivirus software. The software is updated regularly and virus detection is monitored by the Academy's technician.

13. Filtering

13.1 Whilst filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.

13.2 The action will include:

13.2.1. Making a note of the website and any other websites linked to it;
13.2.2. Informing the computing leader and Headteacher;
13.2.3. Logging the incident;
13.2.4. Informing the Internet Service Provider so that the website can be added to the content filter if appropriate;
13.2.5. Discussion with the pupil about the incident, and how they might avoid similar experiences in future
13.2.6. Parents will be informed where necessary.

13.3 The Academy will work with the local authority, CLEOPS and our Internet Service Provider to ensure systems to protect pupils and staff are effective and appropriate.

13.4 Pupils or staff who deliberately try and access unsuitable materials will be dealt with in accordance with the Academy's discipline policies for pupils and staff.

14. Emerging Technologies

14.1 Emerging technologies and resources will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is permitted.

15. Online Bullying (Cyberbullying)

15.1 Online bullying and harassment via Instant messaging, chat rooms, social networking sites etc. are potential problems that can have an effect on the wellbeing of pupils and staff alike.

15.2 Our Academy has a range of strategies and policies to prevent online bullying, outlined in various sections of this policy. These include:

15.2.1. No access in the Academy to public chat-rooms, instant messaging services and social networking sites;
15.2.2. Pupils are taught how to use the internet safely and responsibly which includes how to identify and respond to 'cyberbullying';
15.2.3. Pupils are taught how and where to report incidents that make them feel unhappy or worried;
15.2.4. As with any form of bullying, we encourage pupils to discuss with staff any concerns or worries they have about online bullying and harassment.
15.2.5. Reported incidents of cyberbullying will be followed up and recorded: Appendix 2.

16. Handling Incidents

16.1. At Howbridge there is a strict monitoring and application of the on-line safety policy and a differentiated and appropriate range of sanctions. We expect all members of the school to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's processes.

16.2. Support is actively sought from other agencies as needed (i.e. Vine Trust, LA, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police)

16.3. Any reported incident, even if it occurs outside of school hours, will be investigated in the first instance by the e-Safety Officer.

16.4. Records of the incident will be kept securely by the e-Safety Officer or Designated Safeguarding Lead as appropriate and in line with GDPR rules: Appendix 2

16.5. Parents/Carers are specifically informed of on-line safety incidents involving young people for whom they are responsible.

16.6. The police or relevant agency will be contacted if it is deemed to be a criminal offence

16.7. The Police will be contacted and legal advice sought if one of our staff or pupils receives on-line communication that we consider is particularly disturbing or breaks the law

16.8. We will immediately refer any suspected illegal material to the appropriate authorities

16.9. Monitoring of incidents will be reviewed regularly by our Designated Safeguarding Lead and/or Deputy Headteacher

17. Authorising Internet Access

17.1 All staff must read and sign the 'Acceptable ICT Use Agreement' as part of the Code of Conduct.

17.2 Howbridge will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

17.3 Parents are asked to sign and return a consent form when their child starts at Howbridge.

16. Review

16.1 There will be an annual review of this policy by the Trust Board and/or Howbridge Church of England Junior School

16.2 Next Review Autumn 2021

Appendix 1:Roles and responsibilities

Role	Key Responsibilities
Headteacher: **Mrs Lisa Dale** Assistant Headteacher: **Damon Howlett**	• Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (ECC) guidance • To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. • To take overall responsibility for online safety provision • To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling – see GDPR Policy • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. Essex services • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • To be aware of procedures to be followed in the event of a serious online safety incident • Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised • To receive regular monitoring reports from the Online Safety/Computing Subject Lead through our Team 2 (STEM) • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. network manager • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety via the termly HT update • To ensure school website includes relevant information – see Website Policy
Online Safety Officer: **Andrew Eaves** Designated Child Protection Lead: **Michelle Hibbs**	• Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents • Promote an awareness and commitment to online safety throughout the school community • Ensure that online safety education is embedded within the curriculum • To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs

Role	Key Responsibilities
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To ensure that online safety incidents are logged as a safeguarding incident, where appropriate • Facilitate training and advice for all staff and class digital leaders • Oversee any pupil surveys / pupil feedback on online safety issues • Liaise with the Local Authority and relevant agencies e.g. ZenZero • Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online • To approve the Online Safety Policy and review the effectiveness of the policy • To support the school in encouraging parents and the wider community to become engaged in online safety activities
Computing Curriculum Leader: **Andrew Eaves**	• To oversee the delivery of the online safety element of the Computing curriculum • Ensure eSafety is progressive and meets the current needs of pupils
Network Manager/technician: **Andrew Eaves**	• To report online safety related issues that come to their attention, to the Online Safety Coordinator and/or Designated Child Protection Lead • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis • That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher To ensure appropriate backup procedures and disaster recovery plans are in place • To keep up-to-date documentation of the school's online security and technical procedures

Role	Key Responsibilities
Teachers: **See website for list of current staff**	• To embed online safety in the curriculum • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff, volunteers and contractors: **See website for list of current staff**	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement, and understand any updates **annually**. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Agreement when joining the school. Acceptable use agreement to be re-read to pupils every September. • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school • To contribute to any 'pupil voice' / surveys that gathers information of their online experiences

Role	Key Responsibilities
Parents/carers	• To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren annually. • to consult with the school if they have any concerns about their children's use of technology • to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images
External groups including Parent groups	• Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school • to support the school in promoting online safety • To model safe, responsible and positive behaviours in their own use of technology.

Howbridge Chruch of England Junior School
E-SAFETY CONCERN

Name of child:		Date of report:
DOB:		Date of incident:
Person making the referral:		Status:
Time and location:		
Referred to SLT: YES/NO	Member of SLT:	Signed:
Incident:		
At Risk of Radicalisation? Yes	No	Not sure
Victim:		Other children involved:
Resolutions: (What are we going to do?)		
Outcome		
Police number (if applicable)		
Signed: _____ Date: _____ Designated E-safety Officer		
Response from parent, if appropriate Circle: Mother, father, other _____		

Shared with other staff:						
Social worker	HT	DHT	AHT	PSA	DSL	Other-specify

Appendix 3: Staff ICT Acceptable Use Agreement

The agreement below is an overview of the acceptable use, by staff, of ICT at Howbridge Church of England Junior School. We have an acceptable use agreement to ensure staff are aware of their responsibilities when using ICT. The e-safety and acceptable use policy explains the provision for e-safety throughout the school.

How staff use school ICT

School ICT equipment, including the internet, should be used for school related purposes. Personal use is accepted on the provision usage is in accordance with this agreement, the e-safety policy and deemed reasonable by the deputy or head teacher.

When ICT equipment is to be used, which is not at a fixed location, it is to be booked out using the equipment booking register found in the Computing Room. It is the responsibility of the person returning this equipment to ensure that it is secured safely in the Computing Room.

If laptops, iPads or other mobile devices are to be taken off site this must be agreed by the headteacher or network manager, this is so we know exactly which piece of equipment is where at any time. County guidance is that laptops and other mobile devices are not to be left in cars unattended.

Child safety

It is our responsibility to educate and support our pupils to use electronic devices and the internet safely. We also have a responsibility to report to the e-safety officer (Computing subject leader, Andrew Eaves) any e-safety issues which will be followed up, recorded and acted upon.

Social Networking

Social networking sites must not be accessed in school hours, by staff using the schools facilities, including Wi-Fi. Social networking can be accessed for educational purposes where permission is granted by the deputy or head teacher. e.g. Twitter account to report school sports or snow days, class blog to share children's work. If social networking is to be used age restrictions are to be upheld.

School related business is not to be discussed using social networking; reasonableness is expected when using 'private' or 'direct messaging' as is stated in the Code of Conduct. As a member of the school community we have a responsibility for upholding the Code of Conduct, which states use of social networking must not adversely affect the reputation of the school or bring the school into disrepute.

Befriending of pupils and ex-pupils from our school who are (with the exception of family members) under the age of 18 is not advisable. Befriending of parents is acceptable but discussions of school related business or posting any comments or actions that could adversely affect the school is not acceptable.

E-mail

All e-mails involving school business are to be sent and received using the allocated school e-mail address, unless exceptional circumstances occur. All e-mails from this account are to include a school disclaimer signature at the bottom of the page which will be attached as a template for all e-mails. Only the office staff, deputy or head teacher can e-mail parents directly regarding school related business. We can e-mail children from our school but only from and to a school e-mail account.

Audio, Video and Photography

Audio, video and photographic files remain the property of the school at all times. These are to be stored on the school server or mobile devices (iPad, cameras). These types of files are to be used for school related business; they can be taken and used off site but you are responsible for safe guarding the files and minimising risks.

Only school equipment is to be used by staff for recording audio, video or photographic files. When attending a trip or visit it is the responsibility of the staff member attending to arrange for a school iPad or another school camera to be taken.

File sharing

File sharing, including the use of removable devices (memory sticks) and cloud based technologies (Dropbox, Onedrive, Google Drive) it is the responsibility of the user to safeguard the information being used and minimise risks. Encrypted memory sticks must be used where pupil or staff data is stored. These are supplied to all Teachers and HLTAs, they can also be supplied to other individuals upon request. Lost data should be reported to the Headteacher as a data breach (GDPR) who will notify the relevant authority.

Remote access

We are working towards being able to remotely access the school network from any location but it will be the responsibility of the user to safeguard the information being used and minimise risks. You must ensure that the device in which you are accessing the school network from is up to date with its latest anti-virus and malware software.

The school has the legal responsibility to comply with GDPR

Staff should take responsibility for making sure that they are only saving data for the amount of time they need it and can justify the data they hold. Personal or sensitive data being worked on at home will not be stored on a personal device but will be saved to an encrypted source (e.g. OneDrive or USB). Reasonable measures should be taken to keep data secure (encrypted USB, locking my computer when out of the room etc.). I understand that the staff share (Teacher Drive) is not an encrypted storage area and as such, sensitive data should not be saved here. Instead, it should be emailed to the required staff using the confidential email system we have set up.

Personal Devices

When at school, whilst children are on site (8:45-3:15), personal devices such as mobile phones, tablet computers and laptops should not be used for personal use during direct contact with pupils (teaching times), other than in staff areas e.g. staffroom, office areas. In an attempt to minimise the risk of a data breach, personal mobile phones must not be connected to the school Wi-Fi. Exceptional circumstances to this should be discussed with the deputy or Headteacher in advance. Personal tablets and laptops can be used for educational purposes but you must ensure that they are free from virus and malware if they are to be connected to the schools network. Please refer to the above section regarding audio, video and photography.

If you have any queries, are unsure of anything or do not have a definitive answer for, please seek advice from Computing Subject Leader or the Headteacher before proceeding. Any breaches of this agreement, could lead to action under the Disciplinary procedure, including dismissal in serious cases.

I confirm that I have read and understood the above.

Signed …… Date ……

Name (please print) ……

Appendix 4: Pupil Acceptable Use Agreement

These are the rules I agree to follow when using any digital technology:

- I will ask permission from a teacher before using ICT equipment and will use only my own login and password.
- Where I am given my own account login to access Google Apps, TT Rockstars, Scratch or any other internet based program, I will keep my password safe.
- I understand that I am not allowed to tell anyone else my passwords other than my Parent/Carer.
- If I lose my password or home-school book I must tell an adult, so my password can be changed.
- To protect myself and other pupils, if I see anything I am unhappy with or receive messages I do not like, I will immediately minimize the page and tell a teacher or adult.
- I will not access other people's files or send pictures of anyone without their permission.
- I will not use other people's devices or accounts.
- I will not bring CDs or memory sticks into school unless I have permission and they have been checked to ensure that they are virus free. I am not allowed to copy any files to a personal memory stick.
- I will only e-mail people I know, or that my parent/teacher has approved and the messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone I have met online.
- When I am using the internet to find information, I will check that the information is accurate as I understand that the work of others may not be truthful.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- I will not use my mobile phone in school for any reason. If I do bring my phone to school with me I will follow the school's Mobile Phone Policy.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- If I am involved in incidents of inappropriate behaviour that involve members of the school community (e.g. cyber-bullying, using images/information without permission), the school will take action according the Behaviour Policy.
- I understand that if I do not follow these rules I may not be allowed to use ICT in school and my parents/carers may be contacted

I have read and understood these rules and agree to follow them:

Name:
Class:
Signed:
Dated:

Parent / Carer Countersignature

As the parent / carer of the pupil:

- I know that my child has signed this Acceptable Use Agreement and has received, or will receive, e-Safety education to help them understand the importance of safe use of digital technology– both in and out of school.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.
- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the Internet.
- I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.
- I will encourage my child to adopt safe use of the Internet and digital technologies at home and will inform the school if I have concerns over my child's e-Safety.

Name of Parent:

Signed:

Dated: