E-Safety Policy

MOUNT
BARLBOROUGH HALL
EDUCATING MEN AND WOMEN FOR OTHERS SINCE 1842

Policy written by – H McLoughlin
Policy Date – August 2023
This Policy is for Barlborough Hall School
Linked Policies – Acceptable Use Policy, Anti Bullying Policy, Behaviour Policy, Complaints Policy, Safeguarding Policy, Social Media Policy
Review date August 2024

Mount St Mary's College
Educating Men and Women for Others since 1842
Telephone: 01246 433388
Email: headmaster@msmcollege.com
Address: College Road, Spinkhill, Derbyshire, S21 3YL

Barlborough Hall School
Educating Men and Women for Others since 1842
Telephone: 01246 810511
Email: headteacher@barlboroughhallschool.com
Address: Barlborough Park, Chesterfield,S43 4ES

Contents

Introduction and Overview

This policy deals with how members of the school community, staff and pupils, use electronic data and information regardless of its format whether on their own devices or those provided by the school.

At Mount St Mary's College and Barlborough Hall School a common spirit underpins teaching and learning, the broad curriculum and the entirety of school life. Our mission, inspired by the Jesuit vision and Ignatian characteristics of education, is to nurture well rounded, well-educated and mature men and women of conscience, compassion and competence who will follow the example of Christ as "Men and Women for Others".

We, therefore, in pursuit of excellence expect the best from everyone, aim for the highest standards in all things and set ambitious targets for both students and staff.

Proclaiming that we are all God's creation, made in His image, we insist on respect for the dignity and potential of everyone. We value everyone; are ambitious for everyone; look for, and seek to develop, everyone's talents.
This e-safety policy has at its core a love for justice, a hatred of unfair treatment or discrimination, a special concern for the vulnerable and helpless and a resolution to protect children against abuse of any kind.

It is the duty of the schools to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse, taking into consideration the age of the pupils.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used **in** and outside of school include:

Websites;

Email and instant messaging;

Blogs;

Social networking sites;

Chat rooms;

Music / video downloads;

Gaming sites;

Text messaging and picture messaging;

Video calls;

Podcasting;

Online communities via games consoles; and

Mobile internet devices such as smart phones and **tablets.**

This policy, supported by the Acceptable Use Policy (for all staff, visitors, pupils and parents), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

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

At Mount St Mary's College and Barlborough Hall School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy and the Acceptable Use Policy (for all staff, visitors, pupils and parents) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought onto school premises (personal laptops, tablets, smart phones, etc.).

1.1 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced in the Anti bullying policy.
- Ensure 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.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community (not exclusive to our pupils) can be summarised as follows:

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Content validation: how to check authenticity and accuracy of online content

Contact

- Instant messaging
- Social media apps – Instagram, snapchat, facebook (not exhaustive)
- Grooming
- Sexting
- Cyber-bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of the School community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of 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 cyber-bullying, 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 of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

1.2 Roles and responsibilities

The Senior Leadership Team and IT manager have responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

We believe that it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

Role	Key Responsibilities
Head Teacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident. • To receive monitoring reports from the IT Management • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
	• Promotes an awareness and commitment to e-safeguarding throughout the school community
	• Ensures that e-safety education is embedded across the curriculum
	• Liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• Facilitates training and advice for all staff
	Lliaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers

Role	Key Responsibilities
	• potential or actual incidents of grooming • cyber-bullying and use of social media
Governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the e-safety incident logs, filtering / change control logs
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum

Role	Key Responsibilities
Network Manager/technician	• To report any e-safety related issues that arises, to the Headteacher. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • To ensure the school's policy on web filtering is applied and updated on a regular basis • That he/she keeps up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation/ action/sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • 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

Role	Key Responsibilities
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (KS2 it would be expected that parents / carers would sign on behalf of the pupils) • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • 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 know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Role	Key Responsibilities
	• To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home
Parents/Carers	• To support the school in promoting e-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 • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

1.3 How the policy is communicated to staff, pupils, parents, community

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/ staff policy file
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

New staff receive information on e-Safety and Acceptable Use policies as part of their induction. All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's Designated Safeguarding Lead. See Appendices

1.4 Complaints

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- interview/counselling by tutor / Key Stage Co-ordinator / Senior Management / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system,

- referral to outside services/ Police.

The Headteacher acts as first point of contact for any complaint. Any complaint about staff misuse is also referred to the Headteacher.

Complaints of cyberbullying are dealt with in accordance with our Anti Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.

As with all issues of safety, if a member of staff, a pupil, a parent or carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Headteacher in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded centrally and reported to the school's Designated Safeguarding Lead, in accordance with the school's Child Protection Policy.

1.5 Review and Monitoring

The Headteacher will be responsible for document ownership, review and updates.
The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
The e-safety policy has been written by the Headteacher and Computing co-ordinator and is current and appropriate for its intended audience and purpose.
There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

Education and Curriculum

2.1 Pupil e-safety curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

We have a clear, progressive e-safety education programme as part of the Computing curriculum. It is built on e-safeguarding for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience.

2.2 Educating pupils about online safety

In EYFS & Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private

- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

- Understand the impact of their digital footprint

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them

- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met

- How information and data is shared and used online

- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)

- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

3. Incident management

3.1 Incident Management

There is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are positive and there is rarely need to apply sanctions.

All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.

Support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues.

We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

3.2 Cyberbullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes PHSRHE education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on safe internet use and online safeguarding issues including cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected. In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

3.3 Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or over Isams/Teams.This policy will also be shared on our school website for parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the Senior Leadership team.

4 Managing the ICT Infrastructure

4.1 Internet access, security (virus protection) and filtering

The school has the educational filtered secure broadband connectivity through the which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
USO user-level filtering is used where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;

The approved systems is used to enable secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

Websites are reviewed before use (where not previously viewed or cached) and staff are encouraged to use the school's Learning Platform as a key way to direct students to age / subject appropriate web sites

4.2 Network management (user access, backup)

- Uses individual, audited log-ins for all users
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Storage of all data within the school will conform to the UK data protection requirements
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

- Staff access to the schools' management information system is controlled through a separate password for data security purposes;
- 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 as these have far less security restrictions and inappropriate use could damage files or the network;
- 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;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed.

- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / approved electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school *e.g. teachers access their area / a staff shared area for planning documentation via a VPN solution / RAv3 system;*
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files;
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, that complies with external Audit's requirements;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All computer equipment is installed professionally and meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

4.3 Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers);
- not write passwords down; and
- should not share passwords with other pupils or staff.

Due to the age of our pupils, The Computing Co-ordinator has a record of passwords - though it is always stimulated that 'passwords' should not be shared; this is to ensure pupils are able to access their school logins at all times. A yearly format is followed at Barlborough Hall School to encourage strong passwords and changing regularly.

This also allows access to pupil work to encourage 'paperless' lessons, with the exception of assessment pieces of work.

4.4 Use of Email and internet

Staff

- Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching or in front of pupils. Such access may only be made from personal devices whilst in staff-only areas of school.
- When accessed from personal devices or off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.
- There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored.
- Staff must immediately report to IT Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any online communications must not either knowingly or recklessly:
  - place a child or young person at risk of harm;
  - bring the name of school into disrepute;
  - breach confidentiality;

- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
- making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- use social media to bully another individual; or
- post links or material which is discriminatory or offensive.

4.5 School Website

The School website is maintained by staff at Mount Saint Mary's College and any uploading of information is restricted to them.

The school web site complies with the statutory DfE guidelines for publications;

Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;

The point of contact on the web site is the school address, telephone number and or email:

Home information or individual e-mail identities will not be published;

Photographs published on the web do not have full names attached;

We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

We do not use embedded geodata in respect of stored images

We collate data from parents for external permissions.

4.6 Social Networking

School staff will ensure that in private use:

No reference should be made in social media to students / pupils, parents / carers or school staff

They do not engage in online discussion on personal matters relating to members of the school community

Personal opinions should not be attributed to the *school.*

Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Please read our Social Networking policy for further Guidance.

4.7 Video Conferencing

School **o**nly uses video conferencing for connection to our 'Companion School' in Makumbi.

Parents can now choose to use our secure Teams network for video conferences at the request of the teacher/parent especially for Parents Evenings.

4.8 Online Safeguarding Guidance Use of technology for online / virtual teaching

All staff at Barlborough Hall School use Microsoft Teams for online / virtual teaching. This has been agreed by all stakeholders for its appropriate level of security. Wherever possible, staff should use school devices and contact pupils only via the pupil school email address / log in. This ensures that the setting's filtering and monitoring software is enabled. Virtual lessons should be timetabled and senior staff, should be able to drop in to any virtual lesson at any time – the online version of entering a classroom. Staff engaging in online learning should display the same standards of dress and conduct that they would in the real world; they should also role model this to pupils and parents.

The following points should be considered:

- think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred
- staff and pupils should be in living / communal areas – no bedrooms
- filters at a child's home may be set at a threshold which is different to the school
- resources / videos must be age appropriate – the child may not have support immediately to hand at home if they feel distressed or anxious about content. (Reference to Remote learning policy).

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary.

Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately.

Staff, parent and pupil AUPs should clearly state the standards of conduct required. If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with a senior member of staff and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details. All parental contact is recorded on CPOMS and SLT notified.

5 Data storage

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to the school's central server.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

6 Equipment and Digital Content

6.1 Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are permitted to bring in personal devices for their own use. Staff are not permitted to be using mobile phones during lessons or supervision of children.

Personal telephone numbers may not be shared with pupils, parents or carers and under no circumstances may staff contact a pupil, parent or carer using a personal telephone number.

6.2 Pupils

Mobile technologies available for pupil use including tablets, cameras, etc. are stored in locked cupboards. Access is available via the appropriate member of staff. Members of staff should sign devices out and in before and after each use by a pupil.

No personal devices belonging to pupils at Barlborough Hall School should be brought in. Children who travel on the school bus may being in a device for the journey, but this must be switched off in school. We do not take any responsibility for its safe keeping if not handed in. All phone calls on behalf of pupils and parents are directed through the school office.

6.3 Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents or carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g. on social networking sites).

In accordance with guidance from the Information Commissioner's Office, parents or carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), nor should parents or carers comment on any activities involving other pupils in the digital or video images.

Staff and volunteers are allowed to take digital or video images to support educational aims, but must follow this policy and the Acceptable Use Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital or video images 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.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website (see Parent Contract for more information).

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.