C8i

E-SAFETY POLICY

Introduction

This policy covers guidelines and procedures for staff, pupils, parents and visitors at Dolphin School and is designed to protect the well-being of all who are associated with the school.

Background, appropriate use, health and safety

Related Policies

1. Acceptable Use Policy for Staff
2. Acceptable Use Policy for Pupils
3. Acceptable Use Policy for Parents & Visitors
4. Cyberbullying
5. Use of Social Media
6. Taking, Storing and Using Images of Children
7. ICT Incident Referral Flow Chart
8. Extract of Annex C from DfE's KCSIE September 2020
9. BYOD mobile devices, guidelines and disclaimer forms

This policy should be read in conjunction with the following policies, which are on the school's website:

1. Safeguarding Children at Dolphin Policy
2. Anti-Bullying Policy
3. Data Protection Policy (Privacy Notice)
4. Whole School Behaviour Policy

Background

Dolphin School embraces the advantages of modern technology. However, the School is mindful of the potential for issues to occur, for example bullying. It is the duty of everyone - staff, parents and pupils - to work together to ensure that every child in our care is safe. The purpose of this e- Safety policy is to outline what measures the School takes to ensure that pupils work in an e-Safe environment and that issues are detected and dealt with appropriately. This policy applies to matters arising at School and using School systems.

The policy pays regard to:

- Keeping children safe in education (publishing.service.gov.uk) (2020), particularly Annex C on online safety (extract is in Appendix 8 below).
- UK Council for Child Internet Safety UCCIS
- Department for Education document on Sexting in Schools and Colleges

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young pupils and their personal safety. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

This policy acknowledges that the use of technology must be in line with fundamental British values.

Communicating about e-Safety with Staff, Pupils, Parents and Visitors

Staff to undergo regularly updated safeguarding training which is integrated, aligned and considered as part of the overarching safeguarding approach. We recognise that the active management of hardware, software and connectivity is vitally important and that teachers and parents have a part to play in the safeguarding and protection of pupils. For this reason our policy is available on our school website and is reviewed annually. E-safety is regularly discussed with pupils in lessons and assemblies, and staff and parents are kept informed of the latest advice, with occasional training, booklets and information evenings as appropriate.

We have Acceptable Use Policies (AUPs) for Staff, Pupils, Parents and Visitors - See Appendix 3, 4 & 5. These give clear guidance for all users on the use of technology in the classroom and beyond. They also make clear reference to permissions, restrictions and agreed sanctions. Staff, pupils, parents and visitors have to agree to the relevant AUP as part of their access process.

Pupils are taught about internet safety mainly in Computer Studies lessons, but also in assemblies, mentoring sessions, as well as in PSHE lessons. They are made aware of the dangers of using certain forms of social media and how to protect themselves online. The school works with a number of agencies to develop the best program of study including the ThinkUKnow programme developed by the Child Exploitation and Online Protection (CEOP).

Further Information and Support

The following provides a useful starting point:

www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org

www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
https://educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
Prevent Duty – see school policy on Safeguarding Children at Dolphin

Identifying Incidents

Reporting of incidents is actively encouraged and support is provided through the pastoral system. Incidents are rare but are dealt with immediately and parents are informed. The Anti-Bullying Policy is clear about what is not acceptable and the Whole School Behaviour Policy and AUPs clearly outline sanctions. Staff have access to an e-Safety Incident Referral Flow Chart (Appendix 7) which outlines the way an incident should be reported, managed or escalated. Trends in incidents are also discussed and recorded at Pastoral Care meetings with Heads of Section.

Filtering and Monitoring Inappropriate Content

Through its infrastructure and technical provision the School has put in place safeguards to filter and monitor inappropriate content. This also fulfils our responsibilities under the PREVENT strategy (see Safeguarding policy). A web-filter monitors and reports to the Head of IT via TriComputers, our IT support company. The head of IT and Computer Studies also uses AB Tutor, classroom management software, to monitor pupil use of the internet and keep a log of incidents, which are regularly checked and reported to Heads of Section.

Roles and Responsibilities for Online Safety and Links with the Child Protection, Safeguarding and Welfare Policy

Head of IT and Computer Studies	• Leads the development of the e-Safety education programme for pupils and staff • Manages a parental awareness programme for e-Safety • Liaises with the DSL to deal with e-Safety breaches from reporting through to resolution in conjunction with the Heads of Section. • Works with the IT support company and Leadership Team to create, review and advise on e-Safety and AUPs.
IT Support Company, in liaison with Head of IT	• Ensures that the best technological solutions are in place to ensure e-Safety whilst still enabling pupils to use the system effectively in their learning • Ensures that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a secure and robust manner. In addition, secures and preserves evidence of any e-safety breach • Checks and audits all systems to ensure that no inappropriate data is stored or is accessible • Maintains a log of all e-Safety issues • Reports any e-safety-related issues that arise to the Head of IT • Keeps up-to-date documentation of the School's e-safety and technical procedures. • Monitors systems which track pupil internet use to detect e-Safety breaches • Assists in the resolution of e-Safety issues with the Head of IT and other members of staff.
All staff	• Monitor and report any suspected misuse or problem immediately

	• Model safe, responsible and professional behaviours in their own use of technology; ensuring that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms such as personal email, text, mobile phones, personal social media.
Head / Deputy Head Pastoral / (DSL)	• Manage any disciplinary procedures for pupils which arise as a result of them not following the e-Safety Policy • Work with the Head of IT to ensure that the e-safety policy is kept up-to-date and that it is implemented.

The Management of Personal Data

The School takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff may only take information off site 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 devices. Instead staff should securely use remote access tools provided by the school (such as Remote Desktop Connection, Office 365 and SchoolBase Online).

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

Policy Review

Lead Author: Head of IT and Computer Studies
Review Date: 1 February 2022

ACCEPTABLE USE POLICY (AUP) for Staff

3.1 Overview

Dolphin School is committed to protecting its employees, pupils and the wider school community from illegal or damaging actions by individuals or groups, whether executed knowingly or unknowingly.

IT systems are provided to enhance the quality of education provided at Dolphin School, both directly in the form of teaching and open learning and in the form of administrative tools.

Effective security is a team effort requiring the active participation and support of every member of staff, pupil and affiliate who deals with information and/or information systems. It is therefore the responsibility of everyone at Dolphin School to understand this policy and to conduct their activities accordingly as it reflects the interests of the whole community. These rules are in place to protect employees, pupils and the wider school community and to ensure the school fulfils its legal obligations in areas such as Data Protection.

Inappropriate use of hardware and/or software exposes the school to risks including virus attacks, compromise of network systems and services, and legal issues.

On joining the school, new staff are required to read and sign their agreement to this policy.

3.2 General Use and Ownership

Everyone should be aware that the data they create on the school system remains the property of the school. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual Department Heads are responsible for addressing issues concerning the personal use of the school's IT systems where it pertains to that department. If there is any uncertainty, users should consult the Deputy Head or Head of IT & Computer Studies.

Please read these rules carefully and then sign at the end.

1. Computers are provided for you to work on both in the common room and in individual classrooms.
2. Staff may not install any software on the school computers without consultation with the Head of IT/Deputy Head.
3. No food is allowed in the Computer Suite or near any of the computers in the school. Exercise care to avoid drink spillages near PCs in the staff common room or subject rooms.
4. The IT equipment is an expensive resource used by everyone in the school. Please help us to keep it in good working order by reporting any faults to the IT technician.
5. Cameras, flip cameras, video cameras, sat navs and trip phones may be borrowed by staff from the Deputy's study. Please ensure that photos are downloaded to the appropriate photo archive shared drive on the network and the camera is emptied before returning. Laptops, cameras and other school equipment may not be taken home for personal use without permission. Early Years staff should also refer to school policy C23ii EYFS Use of Cameras and Mobile Phones which has regard to the Statutory Framework for the Early Years Foundation Stage Safeguarding and Welfare Requirement: Child Protection (3.4 'The safeguarding policy and procedures must …cover the use of mobile phones and cameras in the setting.')
6. Staff should not take photos of children using their own private equipment. Use only school equipment. If for any reason there is no alternative, best practice is to download photos onto the school photo archive shared drive on the network as soon as is practicably possible and delete them from your equipment.
7. School software may not be taken for personal use.
8. Children may not be allowed to work in the Computer Suite if unsupervised by a member of staff.

Network

1. You will be given your own username and a password to log in to the school network, Office 365 and the school MIS software, SchoolBase. There is also a facility to access the school's network from home.
2. Always save your work to your My Documents folder (on site), or the staff shared drive for departmental work (on site), or online in your OneDrive account (both on and off site), and try to ensure that you practise good housekeeping with your files. Do not download school data to a personal device, including written reports. Use Office 365 for temporary report-writing; delete any report documents once they are on SchoolBase.
3. Please always log off when you have finished your work.

Internet

The Internet can give access to inappropriate information and pictures and we ensure that the children at Dolphin are protected from such information in the following ways:

1. A content filtering software is installed on the school network which is updated regularly and this prevents access to inappropriate websites.
2. Children may not join in "chat rooms" with other users on the Internet.
3. Games may only be played by children if appropriate and with the teacher's permission. Only in special circumstances is this allowed.
4. Any child feeling uncomfortable or upset by anything they discover on the Internet should report it to a teacher immediately. This should be relayed to the Head of IT for checking and recording.
5. If an Internet resource is of a questionable nature, it is the user's responsibility to check with a member of staff to determine if they may or may not access that resource and the staff member's decision is final.
6. Downloading of files is restricted to staff (or children only when under supervision).
7. All staff should be aware that illegal activities are strictly forbidden. This includes: downloading copyrighted material, threatening or obscene material, or material protected by trade secret. Use for advertising or commercial activities of any kind or political lobbying is not allowed.
8. At work, staff should be aware that the internet is a tool that is available as a teaching and learning resource. Priority access in the common room is for staff using this resource.
9. Breaches of Confidentiality - Please note that if you are using a social networking site in or out of work you must not post information about: the school's pupils or parents, your workplace, your employer, your colleagues nor any other information by which the school can be identified. Social networking may only be used outside your contact time with pupils. Social networking sites may be used in the common room, your office or study, but only in the classroom when pupils are not present. The school will monitor the use of computers on the school premises.

Virus Protection

1. Our computers are protected from virus attack and malware as far as is possible.
2. USB memory sticks should not be used to hold sensitive data that might be in breach of GDPR. Either Office 365 or an encrypted device must be used and virus-checked before use.
3. Do not open email attachments from unknown sources or click on unknown or dubious hyperlinks.

E-mail

1. All staff are provided with a dolphinschool.com e-mail account, which you can access at school and at home. Outlook may be used in school to access this locally. Office 365 can also be used either at school or at home for this.
2. E-mails will be investigated if it is felt that there has been misuse.
3. You may not read anyone else's e-mails without their consent.

Website policy

1. Children are only referred to by first names on our web pages, or not at all. Any pictures of children will not be labelled with their full names.
2. Staff will not put information onto the school website without permission from the school, marketing manager or website manager.

3.3 Security and Proprietary Information

1. Users should take all necessary steps to prevent unauthorised access to information held on IT systems at Dolphin School. Extra care should be taken with data that is classified as personal or sensitive under the Data Protection Act 2018 and UK GDPR.
2. Users should keep passwords secure and not share accounts particularly as the failure to do this could allow unrestricted access to sensitive information from outside the school. Passwords need to be compliant with Microsoft's rules on "strong" passwords containing uppercase characters, lowercase characters and numbers or symbols, between 8 and 16 characters in length.
3. Pupils must not be allowed any form of access to an adult user's account.
4. No client devices, including remote access sessions, should be left unattended and unsecured when a user is logged in. To prevent unauthorised access users must either logout or securely lock any client device whenever these are unattended.
5. Information contained on portable school devices (eg laptops) is especially vulnerable and special care should be exercised when taking these offsite.
6. Emails sent from Dolphin School mail servers must have a disclaimer attached stating that any opinion expressed is that of the sender and may not necessarily be the opinion of Dolphin School.
7. Portable devices must be maintained by the School's IT support company. Anti-virus and software updates will be managed automatically.
8. Users must exercise caution when opening e-mail attachments, as these may contain viruses. Unsolicited emails, emails from an unknown source or emails from a known source that seem "out of character" should be treated with extreme caution. If in doubt, deletion, without opening the email, is the safest course of action. IT Support is available to give advice if needed.
9. Copyright of all material must be respected.

- **I have read this Staff AUP above and agree to abide by it**
- **I have also read the school's social media policy and agree to abide by it**
- **I have also read the school's policy on storing, taking and using photographs and agree to abide by it**

Staff Name: _____

Staff signature: _____ Date_____

APPENDIX 4

ACCEPTABLE USE POLICY (AUP) for Pupils

4.1 Introduction and Background

We are proud of the Computer Studies department at Dolphin School. We would like you to use the equipment to develop many different aspects of your education.

This AUP is designed to protect pupils from inappropriate, unsafe or harmful activities in a school context. The school takes its duty of care to pupils very seriously and whilst there are educational benefits to be gained from the use of the Internet, there are dangers that would be irresponsible to ignore.

Unlike with the staff AUP, pupils are not asked to sign their agreement; however the Head of Computer Studies ensures that all teachers in this department discuss the AUP with their classes so that each pupil understands his responsibilities. In addition, internet safety is formally discussed throughout the school in lessons in the week(s) of and surrounding Safer Internet Day (generally in February) each year, and less formally in lessons throughout the year.

4.2 Aims

1. To allow all users to access and use the Internet safely from School.
2. Provide a mechanism by which all users are protected from sites, information and individuals which would undermine the principles and aims of Dolphin School and might harm the well-being of a pupil.
3. Provide rules which are consistent and in agreement with the Data Protection Act 2018.
4. Provide rules which are consistent with the school rules and the acceptable procedures commonly used on the Internet.

4.3 AUP Requirements of Pupils

General

1. Children are not allowed to use any school computers unless supervised by a member of staff.
2. The IT equipment is an expensive resource used by everyone in the school. Everyone should play their part in keeping the equipment in good condition so that others can use it.
3. No food or drink is allowed in the ICT suite or near any of the computers in the school.
4. Computers are provided for you to work on, which may include researching activities, but not games unless permitted by the supervising teacher.
5. Children may not install any software on the computers without permission and supervision, nor connect a memory stick to a school PC or device. (An exception to this is when a pupil has been permitted to bring in a laptop from home – see Laptop Guidelines for Pupils.)
6. Please leave the Computer Studies suite tidy by replacing headphones, tidying excess cables away, pushing the chairs in and taking personal belongings with you.

Network

1. All children are provided with an individual Microsoft user account for Windows. There is also a generic log in for pupils, in the event of a pupil forgetting a password.
2. Children from Year 3 upwards have individual touch-typing accounts.
3. All children have a Purple Mash educational account.
4. Do not share your passwords with anyone. If you forget your password, speak to the Head of IT who can reset your password for you.
5. Always save your classroom work to the Students shared drive in the appropriate class folder.
6. Save any important personal work in the OneDrive area of Office 365.
7. Try to ensure that you file all your documents in an organised way, so that you do not lose them. Do not save unnecessary files on the server as space is limited. If you lose a file, ask for help.

8. As a pupil at Dolphin School you will hold one or more individual accounts, be they with Windows, Purple Mash or other accounts. You are responsible for your individual accounts and must take all reasonable precautions to prevent others from being able to use them. You must not disclose any passwords or login details to anyone other than IT Support.
9. You should only keep school documents on the school system. Staff may have access to the contents of a user's work area for teaching and learning purposes. In addition, persons responsible for running and maintaining the School's IT systems are automatically permitted access to work areas when a breach of the AUP is suspected by a group or individual.

Internet

The Internet offers many resources to students and teachers, both for research and use of online educational software. However, the Internet can give access to inappropriate information and pictures. We ensure that you are protected from such information as outlined below. Please read the following carefully:

1. The school network is protected from malware, viruses and other forms of cyber attack
2. Content-filters are installed on the network which block access to inappropriate websites
3. Games may not be played online unless permitted to do so by your teacher.
4. If you feel at all uncomfortable or upset by anything that you discover on the Internet you should report it to your teacher immediately, likewise any message you receive that is inappropriate or makes you feel uncomfortable, or any knowledge you have about another pupil who is the victim of cyberbullying.
5. Furthermore if you are at all unsure about the nature of the Internet material you are accessing, you must ask your teacher for support before continuing.
6. Downloading of files is only ever allowed under supervision.
7. Advertising and commercial activities are also not allowed on the school computers.
8. You should never purchase anything on-line at school.
9. Use of any social media such as Facebook, WhatsApp, Instagram is not permitted at school.
10. You must not post personal contact information about yourself, including your address, telephone number or school address. This information must not be provided to any individual, organisation or company.
11. You must not use names, photographs or recordings of any member of the school community without approval from the Head.
12. Before you view, upload, download or post any material you will consider carefully the implications and consequences of your actions.
13. Participate in gaining an understanding of E-safety issues and the safe responses from all E-safety sessions.
14. You must respect the rights of copyright owners.

E-mail

1. All children are provided with a dolphinschool.com email account, and from Year 3 up are given instruction in their lessons on the appropriate use of email.
2. E-mails will be investigated if it is felt that there has been a misuse.
3. Your Computer Studies lessons and Internet Safety talks include advice about security, for example not revealing your personal details or others' personal details, home addresses, photographs, personal videos or telephone numbers on the internet or via e-mail.
4. Pupils are responsible for email. Emails should be written carefully and politely.
5. Email with attachment(s) from an unknown source should be deleted and an unsolicited or anonymous email should be reported immediately to the Head of IT.
6. Any sending of messages or images that are rude, vulgar, impolite, insulting or hurtful is strictly forbidden. If you receive any of the above it must be reported to a member of staff.
7. Both the school and IT support company monitor the use of the school devices.

In conclusion, under the terms of the School's AUP, no activity should be undertaken that could bring the school's name into disrepute.

4.4 How the School responds to Issues of Misuse by Pupils

The following are provided for the purpose of example only. Whenever a pupil or staff member infringes the E-safety Policy, the final decision on the level of sanction will be at the discretion of the Head, who is also the DSL.

A pupil's network rights or use of the any device at school will be suspended during any investigation about misuse. Infringements listed below come with sanctions which are categorised in the same three sections, according to our Behaviour Policy. Please refer to policy entitles Promotion of Good Behaviour and Sanctions adopted for Misbehaviour.

A Category A

1. Use of non-educational sites during lessons
2. Unauthorised use of email, messaging or social networking sites in lessons
3. Playing games
4. Accessing another pupil's workstation without serious consequences
5. Unintentional spamming.

Possible low-level sanctions:

- Staff disapproval expressed (Child reminded of expected good behaviour and school rules)
- Removal from classroom (for a short period of time)
- Removal from classroom room and tell form teacher/mentor

B Category B

1. Accidentally accessing offensive material or pornographic material and not notifying staff
2. Sending offensive messages
3. Second offence at Category A or with more serious consequences
4. Accessing another pupil's email or network account
5. Causing damage to equipment.
6. Sending an email that is regarded as harassment or bullying (one-off)

Possible mid-level sanctions:

- Detention given
- Child's name raised in Staff Meeting because of persistent poor behaviour
- Child sent to Head of Section (Upper/Middle/Lower)
- Child sent to Deputy Head
- Parent written/spoken to officially
- Child 'on report' after consultation with Deputy Head/Form Teacher and parents

C Category C

1. Deliberately corrupting or destroying someone's data
2. Violating privacy of others
3. Deliberately trying to access offensive or pornographic material
4. Any purchasing or ordering of items over the Internet
5. Transmission of commercial or advertising material
6 Hacking - any bypassing of the School's security system irrespective of purpose
7 Intentionally introducing a virus to the network
8 Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
9 Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
10 Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, 2018
11 Bringing the school name into disrepute.

12 Serious or wilful damage to equipment
13 Accessing confidential information
14 Accessing another pupil's email or network account with malicious intent.

Possible high-level sanctions:

- Referred to Head of IT, Head of Section (HoS) and/or Deputy Head (Pastoral) or Head
- Child excluded from social interaction with peers outside of the classroom for a period of time
- Parents called in immediately
- Child excluded from lessons and social interactions
- Child suspended
- Child expelled

ACCEPTABLE USE POLICY (AUP) for Parents and Visitors (and pupils on taster days)

- A visiting speaker might require use of a school PC, eg to connect to the internet.
- A parent who has offered to help create Leavers' Yearbooks or slideshows might request access to the school's photo archive folders.
- A prospective pupil might need temporary access to engage in a lesson.

Visitors, parents or prospective pupils needing to use a school PC will be given a guest login, which allows access to the internet and certain allowed folders. It prevents access to confidential or sensitive data. Visitors should apply Dolphin School standards when using computer equipment in school. These standards should include an awareness of Data Protection and Copyright laws.

5.1 Internet Access and Uploading

1. The school's internet connection is filtered so access might be denied to some sites. Seek permission to access sites that are unavailable through the school's normal filtering system. This might not be immediately possible as changes to the filter can take some time.
2. You are responsible for the sites that appear on any machine that you are using. Report any issues to a member of staff.
3. Never upload and install software or updates without permission from the Head of IT.
4. The school's wi-fi is available to parents and guests and only provides filtered access to the internet, the school's network is not compromised.

5.2 If You Use Your Own Equipment:

1. Make sure that it has up-to-date virus protection software installed
2. That you take care with trailing wires
3. That you can identify your equipment
4. Never leave your equipment unattended or in an unlocked room

5.3 Downloading Files or Documents

For all files:

1. Make sure that the USB stick/external hard drive has recently been virus-checked
2. Never transfer files to a school device unless you have permission
3. Make sure that you clearly state the purpose for transferring these files
4. Check to see if the school machine you would like to transfer files from is encrypted as it might automatically encrypt your USB stick/hard disc drive.

5.4 If you take pictures, video or sound files then check:

1. That you have permission to capture these files
2. That the staff/children have all given their permission for these images/voices to be used
3. That if you intend to use these files in a public area (website, blog etc.) or for financial gain that you request this permission in writing or through email.

5.5 If the file contains sensitive personal data such as staff or pupil information:

1. Get this permission in writing or by email. (Note: Where existing service contracts (Network/MIS support) indicate that this type of work will take place permission will not be needed)
2. Use an encrypted memory stick or hard drive
3. Transfer the file only over a secure email connection.

CYBERBULLYING POLICY

Dolphin School expects all members of the School community to treat other people with courtesy and respect. Everyone has the right to be safe and secure, whether at School or elsewhere, and to be protected when vulnerable, so that all may flourish without fear of unfair treatment or harassment.

The School's approach to bullying is clear: it is always unacceptable. It damages children and the School will therefore do all it can to prevent it.

1.1 Cyberbullying

Cyberbullying is an aggressive act carried out by a group or individual using electronic forms of contact against a victim who cannot easily defend themselves, and includes:

1. Bullying by texts or messages or calls on mobile devices
2. The use of mobile phone cameras to take photos or videos which may cause distress, fear or humiliation
3. Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites and social networking sites
4. Hijacking/cloning e-mail accounts
5. Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook, You Tube, Snapchat, Twitter and Instagram.

Cyberbullying is generally criminal in character. The law applies to cyberspace. It is unlawful to disseminate defamatory information in any media including internet sites. Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character. The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

Dolphin School has systems in place to respond to cyberbullying by blocking access to inappropriate web sites, using firewalls, antivirus protection and filtering systems. Where appropriate and responsible, Dolphin School audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, the School reserves the right to take action against those who take part in cyberbullying. We will support victims and, if necessary, work with the Police to detect those involved in criminal acts. The School will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, either in and out of the School. If necessary, the School will use its power of confiscation to prevent pupils from committing crimes or misusing equipment. All pupils are aware they have a duty to bring to the attention of any member of staff any example of cyberbullying or harassment that they know about or suspect.

The wider search powers, included in the Education Act 2011, give teachers powers to tackle cyberbullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

1.2 Sexting

When an incident involving youth-produced sexual imagery comes to a School's attention:

1. The incident should be referred to the designated safeguarding lead (DSL) as soon as possible
2. The DSL should hold an initial review meeting with appropriate School staff
3. There should be subsequent interviews with the child(ren) involved

4. Parents should be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the pupil at risk of harm
5. At any point in the process, if there is a concern a pupil has been harmed or is at risk of harm, a referral should be made to children's social care and/or the police immediately.

1.3 Initial Review Meeting

The initial review meeting should consider the initial evidence and aim to establish:

1. Whether there is an immediate risk to a pupil or young people
2. If a referral should be made to the police and/or children's social care
3. If it is necessary to view the imagery in order to safeguard the pupil – in most cases, imagery should not be viewed
4. What further information is required to decide on the best response
5. Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
6. Whether immediate action should be taken to delete or remove images from devices or online services
7. Any relevant facts about the young people involved which would influence risk assessment
8. If there is a need to contact another school, college, setting or individual
9. Whether to contact parents or carers of the pupils involved.

An immediate referral to police and/or children's social care will be made, if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a pupil has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the pupil's developmental stage, or are violent
4. The imagery involves sexual acts
5. There is reason to believe a pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the pupil is presenting as suicidal or self-harming.

If none of the above applies, then a school may decide to respond to the incident without involving the police or children's social care (the school can choose to escalate the incident at any time if further information or concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and, if appropriate, local network of support.

1.4 Reporting Incidents to the Police

If it is necessary to refer to the local authority or Police, contact should be made through existing arrangements, as outlined in the Safeguarding policy. This may include seizure of devices and interviews with the young people involved.

Searching Devices, Viewing and Deleting Imagery

1.5 Viewing the imagery

Adults should not view youth-produced sexual imagery unless there is good and clear reason to do so. Wherever possible responses to incidents should be based on what DSLs have been told about the content of the imagery.

The decision to view imagery should be based on the professional judgment of the DSL and should always comply with the child protection policy and any other procedures of the school that are in place.

- If a decision is made to view imagery, the DSL would need to be satisfied that:
    i. viewing is the only way to make a decision about whether to involve other agencies (i.e. it is not possible to establish the facts from the young people involved)
    ii. viewing is necessary to report the image to a website, app or suitable reporting agency to have it taken down, or to support the pupil or parent
    iii. making a report is unavoidable because a pupil has presented an image directly to a staff member or the imagery has been found on a school device or network.

If it is necessary to view the imagery, then the DSL should:

1. Never copy, print or share the imagery; this is illegal
2. Discuss the decision with the Head
3. Ensure viewing is undertaken by the DSL or another member of the safeguarding team with delegated authority from the Head
4. Ensure viewing takes place with another member of staff present in the room, ideally the Head or a member of the senior leadership team. This staff member does not need to view the images
5. Wherever possible ensure viewing takes place on School or college premises, ideally in the Head's or a member of the Senior Leadership Team's office
6. Ensure wherever possible that images are viewed by a staff member of the same sex as the pupil in the imagery
7. Record the viewing of the imagery in the School's safeguarding records including who was present, why the image was viewed and any subsequent actions. Ensure this is signed and dated and meets the wider standards set out by ISI/Ofsted for recording safeguarding incidents
8. Further details on searching, deleting and confiscating devices can be found in the Department for Education Searching, Screening and Confiscation advice (Jan 2018)
9. If youth produced sexual imagery has been unavoidably viewed by a member of staff either following a disclosure from a pupil or as a result of a member of staff undertaking their daily role (such as IT staff monitoring school systems) then DSLs should ensure that the staff member is provided with appropriate support
10. Viewing youth-produced sexual imagery can be distressing for both young people and adults and appropriate emotional support may be required.

1.6 Deletion of images

If the school has decided that other agencies do not need to be involved, then consideration should be given to deleting imagery from devices and online services to limit any further sharing of the imagery. The afore-mentioned DfE Searching, Screening and Confiscation advice highlights that schools have the power to search pupils for devices, search data on devices and delete pupil-produced sexual imagery.

However, just as in most circumstances it is not recommended that school staff view imagery, it is recommended that schools should not search through devices and delete imagery unless there is good and clear reason to do so. It is recommended that in most cases young people are asked to delete imagery and to confirm that they have deleted the imagery. Young people should be given a deadline for deletion across all devices, online storage or social media sites.

Pupils are reminded that possession of youth-produced sexual imagery is illegal. They should be informed that if they refuse or it is later discovered they did not delete the image they are committing a criminal offence and the police may become involved. All of these decisions need to be recorded, including times, dates and reasons for decisions made and logged in the safeguarding records. Parents and carers should also be informed unless this presents a further risk to the pupil.

USE OF SOCIAL MEDIA

This policy applies to social networking and electronic communication

6.1 Introduction

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. In addition to the website, the school runs a Twitter feed and Facebook pages both for marketing purposes and communication with current and past parents, staff and pupils. The school has administrative rights over the accounts, monitoring them to ensure the content enhances the school's reputation. Establishing the school's social networking sites in a clear manner will encourage pupils and alumni to use the school sites in preference to alternatives that may be set up.

Our use of social networking applications also has implications for our duty to safeguard children, young people and vulnerable adults. The policy aims to provide a balance to support innovation whilst providing a framework of good practice. Staff have a responsibility to maintain the reputation of the school and the teaching profession. It is important to establish boundaries and ensure appropriate contact with colleagues and pupils. It must be assumed that whatever is written online anywhere cannot be deleted in the future. If pupils see social networking being used responsibly they will be encouraged to emulate this behaviour themselves. Thus, the purpose of this policy is to ensure that:

1. the school is not exposed to legal risks
2. the reputation of the school is not adversely affected
3. our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

6.2 Scope

This policy covers the use of social networking applications by all school stakeholders, including, employees, advisors and pupils. These groups are referred to collectively as 'school representatives' for brevity.

a) The requirements of this policy apply to all uses of social networking applications which are used for any school-related purpose and regardless of whether the school representatives are contributing in an official capacity to social networking applications provided by external organisations.

b) Social networking applications include, but are not limited to:

   1. Blogs, for example Blogger
   2. Online discussion forums, such as netmums.com
   3. Collaborative spaces, such as Facebook
   4. Media sharing services, for example YouTube
   5. 'Micro-blogging' applications, for example Twitter

c) All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equal Opportunities Policy and Internet and Email Policy.

6.3 Use of Social networking sites in worktime

Use of social networking applications in lesson time for personal use only is not permitted, unless permission has been given by the Head.

6.4 Social Networking as part of School Service

All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head first.

1. Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head. However, school representatives must still operate in line with the requirements set out within the policy.

2. School representatives must adhere to the following Terms of Use:

   The Terms of Use below apply to all uses of social networking applications by all school representatives. This includes, but is not limited to public-facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on the school network or not.

3. Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Dolphin School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

4. Terms of Use:

   Social Networking applications

   1. Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
   2. Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns.
   3. Must not be used in an abusive or hateful manner.
   4. Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
   5. Must not breach the school's behaviour/misconduct, equal opportunities or anti-bullying policies.
   6. Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents.
   7. No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with.
   8. Employees should not identify themselves as a representative of the school.
   9. If employment by Dolphin School is a feature of the employee's page or account, it should respect the spirit of this policy.
   10. References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head.
   11. Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

5. Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

6.5 Guidance/protection for staff on using social networking

Broadly, any contact with pupils must adhere to the staff code of conduct and Safeguarding Policy. Colleagues must apply the same high standards of conduct expected in face to face contact to online contact. Specifically:

1. Staff should not interact with pupils, either from within a closed environment e.g. texting from a phone, Instant Messaging, personal email , or from within a semi-closed environment on social networking sites, such as writing on a 'wall' within Facebook or communicating with someone on Twitter.

2. Online interaction within an 'open' online environment, for example Blog comments or wikis, may be appropriate if for educational purposes, but requires professional judgement. If in doubt seek advice from the school. See note below.

3. No member of staff should interact with any ex-pupil from the school on social networking sites who is under the age of 18, as above in points 1 and 2.

4. This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.

5. Where family and friends have pupils in school and there are legitimate family links, please inform the Head in writing. However, it would not be appropriate to network during the working day on school equipment.

6. It is illegal for an adult to network, giving their age and status as a child.

Note

Communications with the majority of pupils will mean discussing academic work; care with wording is advised as the danger for staff is that well-intentioned communication can be misinterpreted, or even altered without the ability to prove what was written in the first instance. Emails sent via school email addresses are logged and stored on the school's servers, thus providing a level of protection that may not be available elsewhere.

Taking, Storing and Using Images of Children Policy

1. **This Policy**

- This Policy is intended to provide information to pupils and their parents, carers or guardians (referred to in this policy as "parents") about how images of pupils are normally used by Dolphin School ("the school"). It also covers the school's approach to the use of cameras and filming equipment at school events and on school premises by parents and pupils themselves, and the media.

- It applies in addition to the school's terms and conditions, and any other information the school may provide about a particular use of pupil images, including e.g. signage about the use of CCTV; and more general information about use of pupils' personal data, e.g. the school's Privacy Notice. Images of pupils in a safeguarding context are dealt with under the school's relevant safeguarding policy.

2. **General points to be aware of**

- Certain uses of images are necessary for the ordinary running of the school; other uses are in the legitimate interests of the school and its community and unlikely to cause any negative impact on children. The school is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

- Parents who accept a place for their child at the school agree under the school's terms and conditions to the school using images of him/her as set out in this policy and/or from time to time if a particular use of the pupil's image is requested. However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example if they are included incidentally in CCTV or a photograph). Parents of Early Years Foundation Stage should note that photographs of their child individually or in groups will be used in the Early Years Learning journal of each pupil.

- We hope parents will feel able to support the school in using pupil images to celebrate the achievements of pupils, sporting and academic; to promote the work of the school; and for important administrative purposes such as identification and security.

- Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the Bursar in writing. The School will respect the wishes of parents/carers (and indeed pupils themselves) wherever reasonably possible, and in accordance with this policy.

- Parents should be aware that, from Year 7 upwards, the law recognises pupils' own rights to have a say in how their personal information is used – including images.

3. **Use of Pupil Images in School Publications**

- Unless the relevant pupil or his or her parent has requested otherwise, the school will use images of its pupils to keep the school community updated on the activities of the school, and for marketing and promotional purposes, including:

- on internal displays (including clips of moving images) on digital and conventional notice boards within the school premises;

- in communications with the school community (parents, pupils, staff, advisors and alumni) including by school email, on the school network and by post;

- on the school's website and, where appropriate, via the school's social media channels, e.g. Twitter and Facebook. Such images would not normally be accompanied by the pupil's full name without permission; and

- in the school's prospectus and magazine, and in online, press and other external advertisements for the school. Such external advertising could include the pupil's first name and in some circumstances the school will seek the parent or pupil's specific consent, depending on the nature of the image or the use.

- on photo-viewing sites such as Snapfish or Slickpic. These are either password-protected or an encrypted link is sent to parents for viewing residential trip or school play photos. These are regularly deleted after a year.

- The source of these images will predominantly be the school's staff (who are subject to policies and rules in how and when to take such images), or a professional photographer used for marketing and promotional purposes, or occasionally a parent or pupil. The school will only use images of pupils in suitable dress and the images will be stored securely and centrally.

4. Use of Pupil Images for Identification and Security

- All pupils are photographed on entering the school and, thereafter, at yearly intervals, for the purposes of internal identification. These photographs identify the pupil by name, year group, house and form/tutor group.

- CCTV is in use on school premises, and will sometimes capture images of pupils. Images captured on the school's CCTV system are used in accordance with the Privacy Notice and CCTV Policy.

5. Use of Pupil Images in the Media

- Where practicably possible, the school will always notify parents in advance when the media is expected to attend an event or school activity in which school pupils are participating, and will make every reasonable effort to ensure that any pupil whose parent or carer has refused permission for images of that pupil, or themselves, to be made in these circumstances is not photographed or filmed by the media, nor such images provided for media purposes.

- The media and other organisations often ask for the full names of the relevant pupils to go alongside the images, and these will be provided where parents have been informed about these visits and either parent or pupil has consented as appropriate.

- However, Dolphin School pupils occasionally perform at public events, such as the Edinburgh (Fringe) Festival, Barcelona Theatre Festival, Woodley Festival. Since it is impossible to prevent members of the public from taking photos of our children and uploading them to social media sites, it is important that trip leaders inform the parents of these children at the trip meeting before the trip, and/or in writing.

6. Security of Pupil Images

- Professional photographers and videographers are DBS checked and do not need to be accompanied while on the school premises. The media (not DBS checked) is accompanied at all times by a member of staff when on school premises. The school uses only reputable professional photographers and videographers and makes every effort to ensure that any images of pupils are held by them securely, responsibly and in accordance with the school's instructions.

- The school takes appropriate technical and organisational security measures to ensure that images of pupils held by the school are kept securely on school systems, and protected from loss or misuse. The school will take reasonable steps to ensure that members of staff only have access to images of pupils held by the school where it is necessary for them to do so.

- All staff are given guidance on the school's Policy on Taking, Storing and Using Images of Pupils, and on the importance of ensuring that images of pupils are made and used responsibly, only for school purposes, and in accordance with school policies and the law.

7. Use of Cameras and Filming Equipment (including mobile phones) by Parents

- Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in school events, subject to the following guidelines, which the school expects all parents to follow:

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the school therefore asks that it is not used at indoor events.

- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.

- Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.

- Parents are reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts. The school will always print a reminder in the programme of events where issues of copyright apply.

- Parents may not film or take photographs in changing rooms or backstage during school productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.

- The school reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.

- The school sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

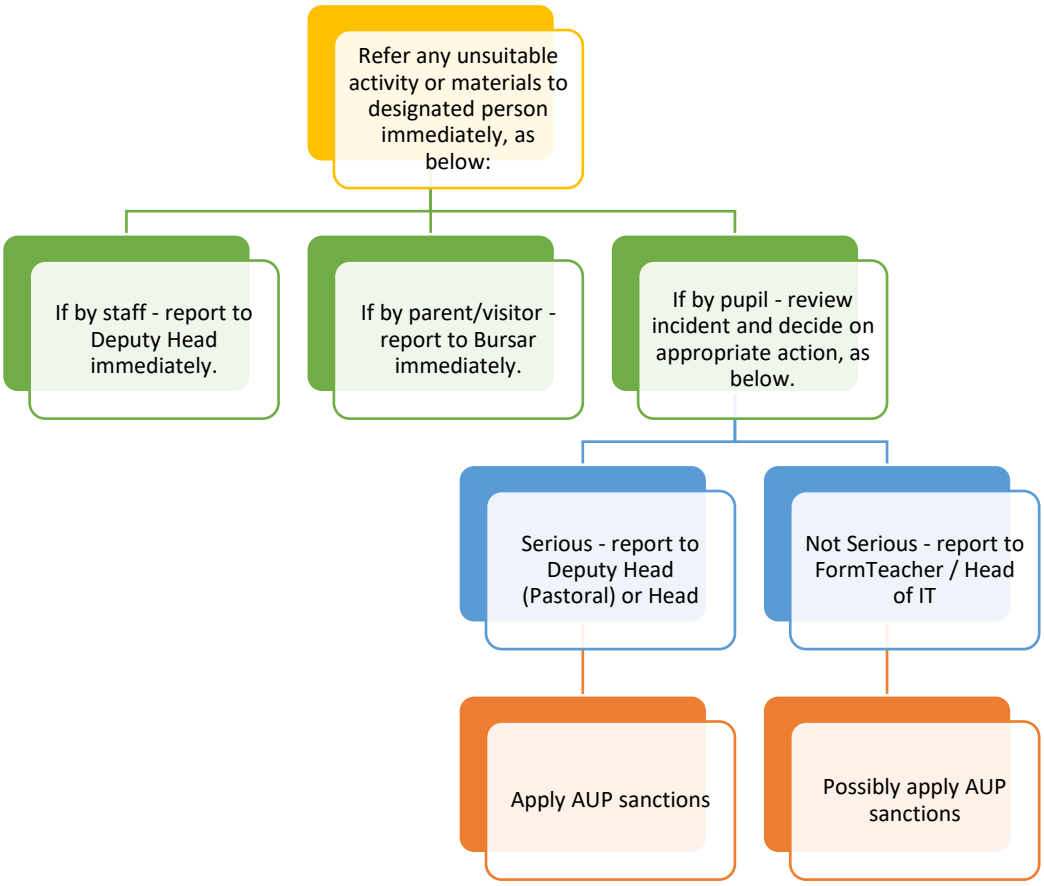
8. **Use of Cameras and Filming Equipment by Pupils**

- All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or any worrying issues to a member of the pastoral staff.

- The use of cameras or filming equipment (including on mobile phones) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

- The misuse of images, cameras or filming equipment in a way that breaches this Policy, or the school's Anti-Bullying Policy, Privacy Policy, e-Safety Policy, IT Acceptable Use Policy for Pupils or Safeguarding Policy is always taken seriously, and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate.

E-SAFETY INCIDENT REFERRAL FLOW CHART



Extract from DfE's 'Keeping children safe in education' (KCSIE) 2020

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate. The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
• contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
• conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Protecting children

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training and the requirement to ensure children are taught about safeguarding, including online safety, that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

For full text see Keeping children safe in education (publishing.service.gov.uk) Annex C: Online Safety

BYOD Policy (Bring Your Own Device)

Guidelines for use of personal laptops, tablets and e-readers

Laptops may only be brought into school with specific permission from the Head. This permission is usually only given to those children who have been deemed to have a specific individual need, where a laptop might provide assistance in their learning.

E-readers may be brought into school by pupils from Years 4 and above for the purpose of quiet reading at approved times. However, the school would encourage printed books.

Parents are required to complete and sign a disclaimer form before a pupil may bring in the device.

Guidelines for laptops in school

1. Remember to bring in your laptop every morning and take it home after school every day. Don't leave it here overnight.

2. Keep your laptop in your form room when not in use during the day.

3. Make sure you charge it at home every evening. You cannot charge it at school unless it is new (proof of purchase required); we have to get all appliances PAT tested annually.

4. If your laptop stops working (eg battery discharged) you will need to revert to pen and paper. Always keep them to hand.

5. Ensure you carry a memory stick with you. Please virus check it first if it is not new. Save any work (that needs printing) onto your memory stick.

6. Create and use a homework folder on your desktop to keep homework recorded. Divide it up into subject folders. This will help you find your files more easily. Do the same on your memory stick.

7. You need to be supervised in the Computer Suite at all times, as normal, so if you are wishing to make use of the school printer please make sure that you only print what is necessary. Check before you print that you won't be printing any extra blank pages. Always try to save toner and paper. To print at school you will need to use a school PC and access the document from your memory stick.

8. Your laptop will not have internet or email access in school so make sure that you do any internet-based research at home.

9. Remember – you are responsible for your laptop, don't lend it to others. It is an important tool for your work.

Laptop disclaimer form for parents

I would like my child to be able to bring his/her laptop/tablet into school for the purpose of assisting with learning.

I understand that the school cannot be held responsible for loss of or damage to this personal property, and that the responsibility for the device remains with the user.

I also agree to the following:

- The user will have a good understanding of its operation as technical support may well not be available;
- The device should be charged and in good order, not charged at school;
- The device will not have an internet connection (excluding wifi);
- The content of the device is appropriate to children of the same age as the user;
- The device is for personal use at school and will not be shared;
- The device will not be a distraction to teachers or pupils or disrupt a class.
- The device may be temporarily removed by a teacher if the above is not adhered to.

Child's name……..

Year group……

Signed by parent…….

Date……..

E-reader disclaimer form for parents

I would like my child to be able to bring his/her e-reader into school for the purpose of reading an e-book at appropriate times of the day.

I understand that the school cannot be held responsible for loss of or damage to this personal property, and that the responsibility for the device remains with the user.

I also agree to the following:

- The user will have a good understanding of its operation as technical support may well not be available;
- The device should be charged and in good order, not charged at school;
- The device will not have an internet connection (excluding wifi);
- The content of the device is appropriate to children of the same age as the user;
- The device is for personal use at school and will not be shared;
- The device will not be a distraction to teachers or pupils or disrupt a class.
- The device may be temporarily removed by a teacher if the above is not adhered to.

Child's name……..

Year group……

Name of parent/guardian

Signed by parent/guardian…….

Date……..