



Datchet St Mary's C of E Primary Academy

Online safety Policy

Reviewed September 2023

Vision

At Datchet St Mary's our vision is 'We are one, we are strongest working together in unity' 1: Corinthians 12 – 14. This vision is at the heart of everything that we do.

Policy produced by Laura Koza

Signed..... Print.....

Date..... Chair/Headteacher/Other.....

To be reviewed: annually

Why does our school need an online safety Policy?

- The exchange of ideas, social interaction and learning opportunities provided by electronic communication technologies are greatly beneficial to all, but can occasionally place children, young people and adults in danger.
- online safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all

members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

- We believe there is a balance to be struck between controlling access to the internet and technology, setting rules and boundaries and educating children and staff about responsible use. Children should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.
- All members of staff need to be aware of the importance of good online safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
- This online safety Policy is essential in setting out how the school plans to develop and establish its online safety approach and to identify core principles which all members of the school community need to be aware of and understand.

Laura Koza is the Computing Lead and Amelia Gilchrist and Nicola Green are the designated safeguarding officers. There is a governor with a specific responsibility for safeguarding and online safety. This Policy is part of many different school policies including the ICT, Child Protection, Anti-bullying and PSHE policies. It has been written by the school, building on government guidance.

The online safety Policy and its implementation will be reviewed annually.

1.2.1 Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide children with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

1.2.2 How does Internet use benefit education?

Benefits of using the Internet in education can include:

- Raised standards of attainment for children
- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;

- Professional development for staff through access to national developments, educational
- Materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and
- Automatic system updates;
- Exchange of curriculum and administration data with the DfE;
- Access to learning wherever and whenever convenient.

1.2.3 How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Children will learn digital literacy skills which are so important in the 21st Century.
- Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research.

1.2.4 How will pupils learn how to evaluate online content?

- Pupils will use age-appropriate tools to research online content, such as using the search engine swiggle.org.uk. (see section 1.3.6)
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

1.3 Managing Information Systems

1.3.1 How will information systems security be maintained?

The school will seek advice from RBWM and ODST regarding SIMS security

Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Devices should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

- Portable media may not be used without specific permission followed by an anti-virus / malware scan. This includes memory sticks. Portable media to be checked for viruses using anti-virus scanning application before use.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- ATMOS technologies will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced by an iTrent authenticator which will require staff members to verify their accounts.
- Staff will sign an equipment agreement (see appendix 5) to ensure any viruses or problems with any equipment are reported promptly so action can be taken to rectify it.

1.3.2 How will email be managed?

Email is central to effective communication throughout the school and all staff are encouraged to access their individual email accounts regularly. All school staff understand they should be using a work provided email account to communicate with parents/carers, pupils and other professionals for any official school business.

- Pupils may only use approved email accounts for school purposes and under the direct supervision of a teacher.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole -class or group email addresses will be used in primary schools for communication outside of the school.
- Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours or for professional purposes.

1.3.3 How will published content be managed?

Publication of any information online should always be considered from a personal and school security viewpoint.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Senior Leadership team will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.

1.3.4 Can pupils' images or work be published?

At Datchet St Mary's Primary Academy the security of staff and children is paramount and the online publishing of children's names with their images is not acceptable. Images of pupils will not be published without the parent's or carer's signed permission.

Pupils also need to be taught the reasons for caution in publishing personal information and images online (see section 1.5.1)

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' first names will be used on the website, with signed parental permission
- Signed permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Signed consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The school has a policy regarding the use of photographic images of children which outlines policies and procedures.

1.3.5 How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location.
- Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy (see appendix 1) and the social media policy (see appendix 2)

1.3.6 How will filtering be managed and monitored

KCSIE 2023 makes it clear that governing bodies should ensure that all staff receive appropriate online safety training, which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, at induction. This training should be regularly updated and refreshed.

1. Identify and assign roles and responsibilities to manage the school's filtering and monitoring systems.

At DSM Miss Green the Head teacher (DSL) and Mrs Gilchrist (DSL) are responsible for ensuring the standards are met. Miss Green and Mrs Gilchrist will work closely with the governors and IT service providers (ATMOS) in all aspects of filtering and monitoring. The schools safeguarding Inset day at the start of a new academic year ensures staff are aware of their role and responsibilities along with the roles and responsibilities of others. Updates are provided as and when necessary to staff in whole staff meetings. Induction training plan

ensures any new staff starting after the Inset training are provided with the relevant up to date training.

Staff are to ensure that any youtube or vimeo videos are played through the <https://safeshare.tv/>. (see appendix 4) This technology reduces any advertisements, annotations, or links to other potentially inappropriate videos to a minimum.. Staff are also to ensure that any online searches carried out by children are done through the search engine [swiggle.org.uk](https://www.swiggle.org.uk) Swiggle is a search engine designed to provide a safer environment, free from adverts. Powered by Google Custom Search, the results are filtered using Google SafeSearch and educational resources prioritised. It also filters the search terms to check that Swiggle is not being used to search for inappropriate content.

2.Review their filtering and monitoring provision at least annually. The Governing body has overall strategic responsibility for meeting the duty to have appropriate/effective filtering and monitoring systems in place. At DSM we review the filtering and monitoring provision annually. The review is conducted by the responsible governor (,)Miss Green, Mrs Gilchrist and Atmos our IT service provider .

3.Ensure their filtering system blocks harmful and inappropriate content without unreasonably impacting teaching and learning. An active and well managed filtering system is an important part of providing a safe environment for pupils to learn. An effective filtering system needs to block internet access to harmful sites and inappropriate content. However, it should not:

1. Unreasonably impact teaching and learning or school administration
2. Restrict students from learning how to assess and manage risk themselves.

Schools need to understand the coverage of their filtering systems and be aware of any limitations it has. This will enable schools to mitigate accordingly to minimise potential harm and meet their statutory requirements under KCSIE 2023 and the [Prevent duty](#).

4.Implement effective monitoring strategies that meet the safeguarding needs at DSM

Monitoring school devices allows you to review user activity. For monitoring to be effective it must pick up incidents urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome. Monitoring strategies may include:

- Physically monitoring by staff watching screens of users
- Live supervision by staff on a console with device management software
- Network monitoring using log files of internet traffic and web access
- Individual device monitoring through software or third-party services.

The software used at DSM **Sophos XG firewall** ensure that any monitoring data is received in a format that staff can understand and that users are identifiable, so concerns can be traced back to an individual, including guest accounts. It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff. Children must therefore have individual log ins when accessing online content so that they can be identified should any inappropriate material be accessed.The DSL Miss Green and Mrs Gilchrist will take lead responsibility for responding to any safeguarding and child protection matters that are picked up through monitoring.

Filtering and monitoring training

KCSIE 2023 makes it clear that governing bodies and proprietors should ensure that all staff receive appropriate online safety training, which includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring, at induction. This training should be regularly updated and refreshed.

Online safety

1.3.7 How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

1.3.8 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

1.4 Policy Decisions

1.4.1 How will Internet access be authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.

1.4.3 How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Computing Coordinator will record all reported incidents and actions taken in the School online safety incident log and other in any relevant areas e.g. Bullying or Child protection log.
- The Designated Child Protection Coordinator will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage online safety incidents in accordance with the school discipline/ behaviour policy where appropriate.

- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or online safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County online safety Officer.
- If an incident of concern needs to be passed beyond the school, then the concern will be escalated to the Designated safeguarding officer to communicate to other schools in RBWM.

1.4.4 How will Online safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All online safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

1.4.5 How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007.

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on antibullying and behaviour.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.
- The Police will be contacted if a criminal offence is suspected.

1.4.6 How will mobile phones and personal devices be managed?

- The use of mobile phones and other personal devices by staff in school will be decided by the school and covered in the school Acceptable Use Policy

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- Any pupils bring in mobile phones or other personal devices should hand them in at the office, switched off, before school and collect them after school.
- Mobile phones and personal devices will not be used during teaching time. They should be switched to silent at all times.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

1.4.6 Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff will use the school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal device as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

1.5 Communication Policy

1.5.1 How will the policy be introduced to pupils?

Teachers will ensure online safety is delivered and matched against the nationally agreed framework 'Education for a Connected World Framework' by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts. **(The Online Safety Provisions Document details where each of these strands should be covered. See appendix 6)** Children will be explicitly taught about online Safety in computing lessons following the NCCE Teach Computing scheme of work as well as using ProjectEVOLVE knowledge's maps and activities to ensure all the safety strands from Education for a Connected World are being covered. Some of these strands are also covered as part of our JIGSAW PSHE scheme. Online Safety should also be discussed as part of every subject whenever pupils are using the internet. Children will also take part in relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week

Children and parents will also sign a code of practice when they start the school (See Appendix 2)

Online safetyOnline safetyOnline safetyOnline safety1.5.2 How will the policy be discussed with staff?

- The online safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

1.5.3 How will parents' support be enlisted?

- Parents' attention will be drawn to the school online safety Policy in newsletters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting online safety at other attended events e.g. parent evenings.

Online safety Policy September 2023

Approved by_____

Date_____

Review Date September 2024

Appendix 1

Datchet St Marys Staff (and Volunteer) Acceptable Use Policy

VISION: Preparing pupils for their futures through real life experiences.

At Datchet St Mary's our vision is 'We are one, we are strongest working together in unity' 1: Corinthians 12 – 14. This vision is at the heart of everything that we do.

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, iPads, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school / academy:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school ICT systems

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school / academy equipment, or the equipment belonging to others..
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name:

Signed:

Date:

Appendix 2

Policy for Social Media

at Datchet St. Mary's C of E Primary Academy

VISION: Preparing pupils for their futures through real life experiences.

At Datchet St Mary's our vision is 'We are one, we are strongest working together in unity' 1: Corinthians 12 – 14. This vision is at the heart of everything that we do.

Introduction to the Policy

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites. The three with the widest use are Facebook, Instagram and Twitter.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance is to protect staff and advise school leadership on how to deal with potential inappropriate use of social networking sites.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

There are four key areas:

- A. The use of social networking sites by pupils outside the school
- B. Use of social networking by staff in a personal capacity
- C. Comments posted by parents/carers
- D. Dealing with incidents of online bullying

- A. The use of social networking sites by pupils outside the school

The school's Acceptable Use Policy (AUP) outlines the rules for using IT in school and these rules therefore apply to use of social networking sites. Social networking sites such as Facebook and Twitter cannot be accessed in school on the school's computer systems due to filters put in place. Social Media sites used by children outside of school are the responsibility of the parent and not the school but the school will take responsibility in educating children about online safety awareness and online bullying. Teachers will ensure online safety is delivered and matched against the nationally agreed framework 'Education for a Connected Work Framework' by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts. (see online safety policy)

Facebook and Instagram are targeted at older teenagers and adults. They have a no under 13 registration policy and recommend parental guidance for 13 to 16 year olds. At Datchet St Mary's we are aware that children will still have access to this social media site and therefore look to educate children of the potential dangers.

B. Use of social networking by staff in a personal capacity

It is possible that a high proportion of staff will have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

Guidelines are issued to staff:

- Staff must never add pupils as 'friends' into their personal accounts (including past pupils under the age of 16).
- Staff are strongly advised not to add parents as 'friends' into their personal accounts.
- Staff must not post comments about the school, pupils, parents or colleagues including members of the Governing Body.
- Staff must not use social networking sites within lesson times (for personal use).
- Staff should only use social networking in a way that does not conflict with the current National Teacher's Standards.
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality.
- Staff should read and comply with 'Guidance for Safer Working Practice for Adults who Work with Children and Young People'.
- Inappropriate use by staff should be referred to the Headteacher in the first instance and may lead to disciplinary action.

C. Comments posted by parents/carers

Parents and carers will be made aware of their responsibilities regarding their use of social networking. Methods of school communication include the prospectus, the website, newsletters, letters, the school facebook page and verbal discussion. School policies and documents provide further information regarding appropriate channels of communication and means of resolving differences of opinion. Effective communication following principles of mutual respect is the best means of ensuring the best learning experiences for the child.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.

Parents should make complaints through official school channels rather than posting them on social networking sites.

Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

D. Dealing with incidents of online bullying/inappropriate use of social networking sites

The school's Anti-Bullying Policy sets out the processes and sanctions regarding any type of bullying by a child on the school roll.

Children will be educated on the impact of online bullying through computing lesson, PSHE and safer internet day.

In the case of inappropriate use of social networking by parents, the Governing Body will contact the parent asking them to remove such comments and seek redress through the appropriate channels such as the Complaints Policy and will send a letter.

The Governing Body understands that, "There are circumstances in which police involvement is appropriate. These include where postings have a racist element or where violence is threatened or encouraged." Furthermore, "Laws of defamation and privacy still apply to the web and it is unlawful for statements to be written...which:

- expose (an individual) to hatred, ridicule or contempt
- cause (an individual) to be shunned or avoided
- lower (an individual's) standing in the estimation of right-thinking members of society or

- disparage (an individual in their) business, trade, office or profession.” (National Association of Headteachers)

Datchet St Mary's C of E Primary Academy

Acceptable Use AGREEMENT FOR PUPILS AND PARENTS

VISION: Preparing pupils for their futures through real life experiences.

At Datchet St Mary's our vision is 'We are one, we are strongest working together in unity' 1: Corinthians 12 – 14. This vision is at the heart of everything that we do.

Introduction

Digital technologies have become integral to the lives of children and young people, both within and outside schools. These technologies are powerful tools, which open-up new opportunities for everyone. They can stimulate discussion, encourage creativity and stimulate awareness of context to promote effective learning. Learners should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly
- I will only visit internet sites that adults have told me are safe to visit
- I will keep my username and password safe and secure and not share it with anyone else
- I will be aware of "stranger danger" when I am online
- I will not share personal information about myself or others when online
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

- I will not send photos or post detailed personal information about myself or other people. (Personal contact information includes your home address, telephone or mobile number, school address, email addresses, etc.)
- I will not meet with someone I have met online without my parent's /guardian's approval and participation
- I will not use internet social networks, online chats, discussion groups or mailing lists that are not relevant to my education or are not age appropriate

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do. (schools may wish to add anything that would not be allowed e.g. online games, file sharing etc.)

I will think about how my behaviour online might affect other people:

- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:

- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, loss of

break/lunch time, suspensions, parents/carers contacted and in the event of illegal activities involvement of the police.

Notification

- o I will tell a teacher immediately about any message I receive that are rude or that upset or worry me
- o I will tell a teacher if someone else is doing something which offends me or is not permitted

Parental responsibilities, including social media

Outside school it is parents' responsibility to provide guidance in their children's use of the Internet. Appropriate use at home will be beneficial to children educationally, and will often be a valuable aid to both homework and school work. We would advise that this use is closely supervised to eliminate access to inappropriate material.

Parents must not post pictures of pupils, other than their own children, on social networking sites where these photographs have been taken at a school event.

Parents should make complaints through official school channels rather than posting them on social networking sites.

Parents should not post malicious or fictitious comments on social networking sites about any member of the school community.

Learner Acceptable Use Agreement Form (Reception/KS1)

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement.

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Name of Learner:

Class:

Signed by learner:

Date:

Signed by Parent/Carer (parental responsibilities):

Learner Acceptable Use Agreement Form (KS2)

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement.

I have read and understand the acceptable use agreement and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Name of Learner:

Class:

Signed by learner:

Date:

Signed by Parent/Carer (parental responsibilities):

Appendix 4

Staff acceptable use agreement of Youtube/Vimeo videos within school

The purpose of this agreement is to ensure all/any content shown to children within school is acceptable, educationally relevant and age appropriate.

All staff will agree

- To use <https://safeshare.tv/> to share the video with children. This technology reduces any advertisements, annotations, or links to other potentially inappropriate videos to a minimum.
- To have watched the clip in its entirety to ensure it is free from any inappropriate pop ups.

I except full responsibility for the video I am showing children and understand that the video has to meet the above criteria

Signed _____ Date _____

Appendix 5

Datchet St Mary's C of E Primary Academy

Equipment

VISION: Preparing pupils for their futures through real life experiences.

At Datchet St Mary's our vision is 'We are one, we are strongest working together in unity' 1: Corinthians 12 – 14. This vision is at the heart of everything that we do.

I _____ *****NAME***** confirm that I have taken temporary possession of the items provided by Datchet St. Mary's C of E Primary Academy listed on the attached sheet.

I accept that this has been provided for educational use only and I will be responsible for ensuring that all downloaded software is safe and from trusted sites only.

The iPad/laptop will be loaded with anti-virus software and it is my responsibility to ensure it is maintained at all times. I will notify the school promptly if there is a problem with any equipment to ensure prompt action can be taken to rectify it.

I guarantee that I will treat these items with the utmost care and in a responsible manner. I will use the case provided for protection at all times. It will not, on any occasion, be left in a car or kept anywhere other than a safe place.

I am responsible for any damage or loss of the iPad/laptop whilst it is in my possession and will ensure arrangements are made to replace any lost item at cost to myself.

It will be returned to the school when requested.

Signed

Date

EYFS Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can recognise that I can say 'no', 'please stop', 'I'll tell', 'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset.	Jigsaw
Online Relationships	I can recognise some ways in which the internet can be used to communicate. I can give examples of how (I might) use this technology to communicate with people I know.	Project Evolve activity
Online Reputation	I can identify ways that I can put information on the internet.	Project Evolve activity
Online Bullying	I can describe ways that some people can be unkind online. I can offer examples of how this can make others feel.	Project Evolve activity Project Evolve activity
Managing Online Information	I can talk about how I can use the internet to find things out. I can identify devices I could use to access information on the internet. I can give simple examples of how to find information (e.g. search engine, voice activated searching)	Project Evolve short activity Project Evolve short activity
Health, Well-Being & Lifestyle	I can identify rules that help keep us safe and healthy in and beyond the home when using technology. I can give some simple examples.	Covered by completing the AUP (acceptable use policy) at the start of the year.
Privacy & Security	I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location) I can describe the people I can trust and can share this with; I can explain why I can trust them.	Project Evolve activity
Copyright & Ownership	I know that work I create belongs to me. I can name my work so that others know it belongs to me.	Ongoing throughout all activities where work is produced.

Y1 Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can recognise that there may be people online who could make me feel sad, embarrassed or upset. If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust and how they can help.	Jigsaw; Celebrating Difference piece 6 – <u>but specific links to online need to be made here.</u> Project Evolve activity could also be used
Online Relationships	I can use the internet with adult support to communicate with people I know. I can explain why it is important to be considerate and kind to people online. I can give examples of when I should ask permission to do something online and explain why this is important.	Jigsaw; Celebrating Difference piece 4 – <u>but specific links to online need to be made here.</u> Project Evolve has 2 activities that could be used to supplement.
Online Reputation	I can recognise that information can stay online and could be copied. I can describe what information I should not put online without asking a trusted adult first.	Project Evolve activity Project Evolve activity
Online Bullying	I can describe how to behave online in ways that do not upset others and can give examples.	Jigsaw; Celebrating Difference pieces 3 & 4 – <u>but specific links to online need to be made here.</u> Project Evolve has 1 activity that could be used to supplement.
Managing Online Information	I can use the internet to find things out. I can use simple keywords in search engines. I know / understand that we can encounter a range of things online including things we like and don't like as well as things which are real or make believe / a joke. I can describe and demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable, worried or frightened.	Project Evolve activity Jigsaw; Relationships piece 4 - <u>but specific links to online need to be made here</u>
Health, Well-Being & Lifestyle	I can explain rules to keep us safe when we are using technology both in and beyond home. I can give examples of some of these rules.	Covered NCCE unit Y1 Technology around us
Privacy & Security	I can recognise more detailed examples of information that is personal to me (e.g. where I live, my family's names, where I go to school). I can explain why I should always ask a trusted adult before I share any information about myself online, belonging to myself or others. I can explain why passwords can be used to protect information and devices.	Project Evolve Activity NCCE unit Y1 digital writing Jigsaw; Relationships piece 4 - <u>but specific links to online need to be made here</u> Project Evolve Activity

Copyright & Ownership	I can explain why work I create using technology belongs to me. I can say why it belongs to me (e.g. "It is my idea" / "I designed it") I understand that work created by others does not belong to me even if I save a copy I can save my work so that others know it belongs to me (e.g. filename, name on content)	Covered in NCCE unit Y1 Technology around us NCCE Y1 IT Digital painting & grouping data
----------------------------------	---	--

Y2 Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can explain how other people may look and act differently online and offline. I can give examples of online issue that might make me feel sad, worried, uncomfortable or frightened. I can give examples of how I might get help.	Jigsaw; Celebrating Difference piece 6 – <u>but specific links to online need to be made here.</u> NCCE unit Y2 pictograms
Online Relationships	I can give examples of how someone might use technology to communicate with others they don't also know offline and explain why this might be risky. (e.g. email, online gaming, a pen-pal in another school / country). I can explain who I should ask before sharing things about myself or others online. I can explain how it may make others feel if I do not ask their permission or ignore their answers before sharing something about them online.	Project Evolve activity
Online Reputation	I can explain how information put online about someone can last for along time. I know who to talk to if I think someone has made a mistake about putting something online. I can describe how anyone's online information could be seen by others.	Project Evolve activity Project Evolve activity
Online Bullying	I can explain what bullying is, how people may bully others and how bullying can make someone feel. I can explain why anyone who experiences bullying is not to blame I can talk about how anyone experiencing bullying can get help.	Project Evolve has 2 short activities that cover these objectives.
Managing Online Information	I can use keywords in search engines. I can demonstrate how to navigate a simple webpage to get information I need (e.g. home, forward, back buttons; links, tabs and sections) I can explain what voice activated searching is and how it might be used (e.g. Alexa, Google Now, Siri) I can explain the difference between things that are imaginary, 'made up', or 'make believe' and things that are 'true' or 'real'. I can explain why some information I find online may not be true. I can explain why some information I find online may not be real or true.	Project Evolve activity Project Evolve Activity NCCE Y2 Digital photography unit
Health, Well-Being & Lifestyle	I can explain simple guidance for using technology in different environments and settings. I can say how those rules/guides can help me.	Covered in NCCE unit Y2 Information technology around us and pictograms

Privacy & Security	I can describe and explain some rules for keeping my information private. I can explain what passwords are and can use passwords for my accounts and devices. I can explain how many devices in my home could be connected to the internet and can list some of those devices.	Project Evolve Activity Project Evolve Activity NCCE Y2 Information technology around us.
Copyright & Ownership	I can describe why other people's work belongs to them. I can recognise that content on the internet may belong to other people.	NCCE Y2 Digital Making Music NCCE Y2 Digital photography unit

Year 3 Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can explain what is meant by the term 'identity' I can explain how I can represent myself in different ways online I can explain ways in which and why I might change my identity online depending on what I am doing online.	1 activity from Project Evolve which covers all three objectives
Online Relationships	I can describe ways people who have similar likes and interests can get together online. I can explain the importance of giving and gaining permission before sharing things online; how the principles of sharing online is the same as sharing offline e.g. sharing images and videos. I can explain what is meant by 'trusting someone online', why this is different from 'liking someone online', and why it is important to be careful about who to trust online including what information and content they are trusted with. I can explain what it means to 'know someone' online and why this might be different from knowing someone offline. I can explain why someone may change their mind about trusting anyone with something if they feel nervous, uncomfortable or worried.	Activity in Project Evolve Activity in Project Evolve Activity in Project Evolve covers these few objectives. Activity in Project Evolve.
Online Reputation	I can search for information about others online. I can give examples of what anyone may or may not be willing to share about themselves online. I can explain the need to be careful before sharing anything personal. I know who I should ask if I am not sure if I should put something online.	Covered by Jigsaw (Relationships Piece 3) Activity in Project Evolve for both these objectives
Online Bullying	I can describe appropriate ways to behave towards other people online and why this is important I can give examples of how bullying behaviour could appear online and how someone can get support.	Covered by Jigsaw (Relationships Piece 3)
Managing Online Information	I can use key phrases in search engines. I can explain what autocomplete is and how to choose the best suggestion. I can explain the difference between a belief, an opinion and a fact.	Covered by NCCE IT unit Y3: stop frame Animation and desktop publishing Activity in Project Evolve

Health, Well-Being & Lifestyle	I can explain why spending too much time using technology can sometimes have a negative impact on me; I can give some examples of activities where it is easy to spend a lot of time engaged (e.g. games, films, videos). I can explain why some online activities have age restrictions, why it is important to follow them and know who I can talk to if others pressure me to watch or do something online that makes me feel uncomfortable (e.g. age restricted gaming or web sites).	Activity in Project Evolve
Privacy & Security	I can give reasons why I should only share information with people I choose to and can trust. I can explain what if I am not sure of feel pressured I should ask a trusted adult. I can describe simple strategies for creating and keeping passwords private. I can describe how connected devices can collect and share my information with others.	Activity in Project Evolve Activity in Project Evolve for both these objectives
Copyright & Ownership	I can explain why copying someone else's work from the internet without permission can cause problems.	Covered by NCCE IT unit Y3: stop-frame Animation

Year 4 Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can explain how my online identity can be different to my offline identity. I can describe the right decisions about how I interact with others and how others perceive me. I can explain that others online can pretend to be someone else, including my friends, and can suggest reasons why they might do this.	Activity in Project Evolve Covered in NCCE IT unit Y4: Photo Editing
Online Relationships	I can give examples of how to be respectful to others online. I can describe strategies for safe and fun experiences in a range of online social environments (e.g. livestreaming, gaming platforms)	Activity in Project Evolve
Online Reputation	I can describe how others can find out information about others by searching online. I can explain ways that some of the information about anyone online could have been created, copied or shared by others.	Activity in Project Evolve
Online Bullying	I can identify some online technologies where bullying might take place and recognise when someone is upset, hurt or angry online. I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat). I can explain why I need to think carefully about how content I post might affect others, their feelings and how it may affect how others feel about them (their reputation).	Activity in Project Evolve Activity in Project Evolve
Managing Online Information	I can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites). I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in-app purchases; pop-ups) and can recognise some of these when they appear online. I can explain that technology can be designed to act like or impersonate living things (e.g. bots) and describe what the benefits and the risks might be. I can explain what is meant by fake news, e.g. why some people	Activity in Project Evolve Activity in Project Evolve Activity in Project Evolve (short task)

	will create stories or alter photographs and put them online to pretend something is true when it isn't. I can describe how fake news may affect someone's emotions and behaviour, and explain why this may be harmful.	Covered by NCCE unit Y4: The Internet
Health, Well-Being & Lifestyle	I can explain how using technology can distract me from other things in both a positive and negative way. I can identify times or situations when I might need to limit the amount of time I use technology and suggest strategies to help me with this.	Activity in Project Evolve (longer session)
Privacy & Security	I can explain what a strong password is and describe strategies for keeping my personal information private, depending on context. I can explain that internet use is never fully private and is monitored e.g. adult supervision. I know what the digital age of consent is and the impact this has on online services asking for consent.	Activity in Project Evolve Activity in Project Evolve
Copyright & Ownership	When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it. I can give some simple examples of content which I must not use without permission from the owner, e.g. videos, music, images.	Covered by NCCE IT unit Y4: Audio production and Photo Editing.

Year 5 Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can explain how identify online can be copied, modified or altered. I can demonstrate responsible choices about my online identity; depending on context.	Project Evolve (2 activities)
Online Relationships	I can explain that there are some people who I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault. I can make positive contributions and be part of online communities. I can describe some of the communities in which I am involved and describe how I collaborate with others positively.	Covered by Jigsaw – Relationships, pieces 2-6 In Summer Term 1
Online Reputation	I can search for information about an individual online and create a summary report of the information I find. I can describe ways that information about people online can be used by others to make judgements about an individual.	Partly covered by Jigsaw – Relationships pieces 2-6 in Summer Term 1 Project Evolve 1 longer session to complement.

Online Bullying	I can recognise when someone is upset, hurt or angry online. I can describe how to get help for someone that is being bullied online and assess when I need to do or say something or tell someone. I can explain how I would report online bullying on the apps and platforms that I use. I can describe the helpline services who can support me and what I would say and do if I needed their help e.g. Childline. I can explain how to block abusive users.	Partly covered by Jigsaw – Relationships pieces 2-6 in Summer Term 1 Project Evolve activity
Managing Online Information	I can explain what is meant by ‘being sceptical’. I can give some examples of when and why it is important to be sceptical. I can explain what is meant by a hoax. I can explain why I need to think carefully before I forward anything online. I can identify ways the internet can draw us to information for different agendas, e.g. website notifications, pop-ups, targeted ads I can describe ways of identifying when online content has been commercially sponsored or boosted, (e.g. by commercial companies or by vloggers, content creators, influencers)	Project Evolve activity x4
Health, Well-Being & Lifestyle	I can describe ways technology can affect healthy sleep and can describe some of the issues. I can describe some strategies, tips or advice to promote healthy sleep with regards to technology. I can explain how and why some apps and games may request or take payment for additional content (e.g. in-app purchases, lootboxes) and explain the importance of seeking permission from a trusted adult before purchasing.	Project Evolve activity – 1 longer session. Related to Jigsaw; Relationships piece 5 (but not specifically sleep)
Privacy & Security	I can create and use strong and secure passwords. I can explain how many free apps or services may read and share my private information (e.g. friends, contacts, likes, images, videos, voice messages, geolocation) with others. I can explain how and why some apps may request or take payment for additional content (e.g. in-app purchases) and explain why I should seek permission from a trusted adult before purchasing. I can explain what app permissions are and can give some examples.	Project Evolve activity Project Evolve activity Project Evolve activity
Copyright & Ownership	I can assess and justify when it is acceptable to use the work of others. I can give examples of content that is permitted to be reused.	Covered in NCCE Y5 Systems and Networks unit.

Year 6 Online Safety Provision

Strand	Objectives	Where covered
Self-Image & Identity	I can describe ways in which media can shape ideas about gender. I can identify messages about gender roles and make judgements based on them. I can challenge and explain why it is important to reject inappropriate messages about gender online. I can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. I know and can give examples of how I might get help, both on and offline. I can explain why I should keep asking until I get the help I need.	Project Evolve activity Jigsaw; Relationships pieces 1 – 6.

Online Relationships	I can explain how sharing something online may have an impact either positively or negatively	Jigsaw; Relationships pieces 5 + 6
	I can explain how sharing something online may have an impact either positively or negatively I can describe how things shared privately online can have unintended consequences for others e.g. screen grab.	Project Evolve
	I can explain that taking/sharing inappropriate images of someone may have an impact for the sharer and others; and who can help if someone is worried about this.	Project Evolve
Online Reputation	I can explain how I am developing an online reputation which will allow other people to form an opinion of me. I can describe some simple ways that help build a positive online reputation.	Jigsaw; Relationships
Online Bullying	I can describe how to capture bullying content as evidence (e.g. screen grab, URL, profile) to share with others who can help me. I can explain how someone could report online bullying in different contexts.	Project Evolve Project Evolve Also supported by Jigsaw
Managing Online Information	I can use search technologies effectively. I can explain how search engines work and how results are selected and ranked. I can demonstrate the strategies I would apply to be discerning in evaluating digital content. I can describe how some online information can be opinion and can offer examples. I can explain how and why some people may present opinions as facts. I can demonstrate strategies to enable me to analyse and evaluate the validity of facts and I can explain why using these strategies are important. I can identify and flag inappropriate content. I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how I might encounter these online e.g. advertising and ad-targeting.	NCCE Y6 Systems & Networks unit Jigsaw; Relationships piece 5 Project Evolve activity
Health, Well-Being & Lifestyle	I recognise and can discuss the pressures that technology can place on someone and how/when they could manage this. I can describe common systems that regulate age-related content (e.g. PEGI, BBFC, parental warnings) and describe their purpose. I can recognise features of persuasive design and how they are used to keep users engaged (current and future use)	Project Evolve activity Project Evolve activity

	I can assess and action different strategies to limit the impact of technology on my health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and exercise).	Project Evolve activity
Privacy & Security	I use different passwords for a range of online services. I can describe effective strategies for managing those passwords. I know what to do if my password is lost or stolen.	Project Evolve activity
	I can describe simple ways to increase privacy on apps and services that provide privacy settings. I can describe ways in which some online content targets people to gain money or information illegally; I can describe strategies to help me identify such content (e.g. scams, phishing).	Project Evolve activity
Copyright & Ownership	I can demonstrate the use of search tools to find and access online content which can be reused by others. I can demonstrate how to make references to and acknowledge sources I have used from the internet.	NCCE Y6 IT Web Design unit