ERASMUS DARWIN ACADEMY

Policy Title:	**Online Safety Policy**
Policy Reference:	E4
Version:	1.6
Member of Staff Responsible:	Headteacher
Date adopted by Governing Body:	February 2026
Date of Review:	February 2027
Date Reviewed:	8 July 2015 23 June 2016 29 November 2016 21 March 2017 22 March 2018 9 April 2019 31 March 2020 (No change) 23 March 2021 5 July 2021 7 March 2023 19 February 2024 7 January 2025 23 February 2026

Change Record

Version	Date	Description
1.1	05/04/22	Changes to Section 12, 14
1.2		
1.3		
1.4	20.2.24	Changes to Section 3.2, 3.4, 3.5, 6.3, 12, Appendix B & D
1.5	7.1.25	Amended the name of the policy to 'Online Safety' instead of 'E-Safety'. Replaced the wording E-Safety with Online Safety
1.6	23/2/26	Addition of misinformation, disinformation and conspiracy theories into Content section in lin with KCSIE 2025 Update of named filtering and monitoring programmes Update to Google's AI name (from, Bard to Gemini)

Erasmus Darwin Academy promotes the safeguarding and welfare of children in its care; all policies support the Safeguarding Policy.

Approved by
Name: Title: Chair of Governors

Date of next review	February 2027

CONTENTS **Page Number**

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating students about online safety 5
5. Educating parents about online safety 5
6. Cyber-bullying 5
7. Sharing nude and semi-nude images 6
8. Acceptable use of the internet in the Academy 7
9. Students using mobile devices in the Academy 7
10. Students using devices offsite 8
11. Staff using work devices outside school 8
12. How the Academy will respond to issues of misuse 8
13. Training 8
14. Monitoring arrangements 9
15. Links with other policies 9

APPENDICES – ACCEPTABLE USE AGREEMENTS

Appendix A - Student ICT Acceptable Use Agreement (Years 7-1)) 10

Appendix B – Student ICT Acceptable Use Agreement (Sixth Form) 11

Appendix C - Staff ICT Acceptable Use Agreement 14

Appendix D - Parent ICT Acceptable Use Agreement 17

Appendix E - Visitor ICT Acceptable Use Agreement 19

Appendix F - Governor ICT Acceptable Use Agreement 20

1. Aims

Our Academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Academy community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This procedure is based on the Department for Education's statutory safeguarding guidance, , Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

Non-statutory guidance from the Department for Education on sharing nude and semi-nude images is available here and is used to support section 7 of this policy.

3. Roles and Responsibilities

3.1 The Local Governing Body

The governing body has overall responsibility for monitoring this procedure and holding the Headteacher to account for its implementation.

The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing body must ensure the Academy has appropriate filtering and monitoring systems in place on Academy devices and Academy networks, and will regularly review their effectiveness. The governing body will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the Academy in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Brendan O'Reilly (Vice Chair of Governors)

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-Academy or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

All governors will:
• Ensure that they have read and understand this procedure
• Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet

3.2. Headteacher

The Headteacher is responsible for ensuring that staff understand this procedure, and that it is being implemented consistently throughout the Academy.

3.3 The designated safeguarding lead (DSL)

Details of the Academy's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the Academy, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy

- Working with the headteacher and governing body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on Academy devices and Academy networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Academy's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the Academy to the headteacher and/or governing body
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Senior IT Technician

The Senior IT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, on Academy devices and Academy networks which are updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at the Academy, including terrorist and extremist material
- Ensuring that the Academy's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the Academy's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this procedure
- Implementing this procedure consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's ICT systems and the internet and ensuring that students follow the Academy's terms on acceptable use
- Following the correct procedures by emailing the Senior IT technician and the DSL if they need to bypass the filtering and monitoring systems for educational purposes

-
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this procedure.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this procedure
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's ICT systems and internet (appendices 1 and 2)
- Read and utilise the information available on the Academy website to promote Online Safety at home.
- Monitor their child's use of social media and ensure they are safe when using the internet.
- Monitor their child's mobile device and online activity, particularly in reference to online hoax material and online challenges.
- Use social media communications appropriately and positively, especially when making reference to the Academy or staff specifically, avoiding situations where negative or derogatory comments are posted in the public domain.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.6 Students

Students should be:

- Aware that by clicking the Accept button on the network's Acceptable Use Agreement (AUA) at login, they are agreeing to be bound by the terms of the AUA.
- Responsible for following the Acceptable Use Agreement while within the Academy as agreed at the beginning of each academic year or whenever a new child attends the Academy for the first time.
- Taught to use the internet in a safe and responsible manner through IT, Computing, PD and other subjects and other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

3.7 Visitors and members of the community

Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this procedure, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4 and Key Stage 5** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

The Academy will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents via our website.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with a member of the Safeguarding Team.

The Academy will let parents/carers know:

- What systems the Academy uses to filter and monitor online use, which is smoothwall ~~and senso~~.

6. Cyber-bullying

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

6.2 Preventing and addressing cyber-bullying
To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The Academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Tutor Period, PD, IT and other subjects where appropriate.
All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding E-Newsletters.

The Academy also has information links available on the website to support parents and carers with Online Safety.

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour for learning policy. Where illegal, inappropriate or harmful material has been spread among students, the Academy will use all reasonable endeavours to ensure the incident is contained.

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

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the Academy rules as a restricted or prohibited item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from a member of SLT.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the Academy or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the Academy complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini ~~Bard~~.

Erasmus Darwin Academy recognises that AI has many uses to help students learn, but may also have the potential to be used to cause harm to others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Erasmus Darwin Academy will treat any use of AI to cause harm or any incident of AI used to target students with our Behaviour for Learning policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the Academy/trust.

AI misuse is also covered in the Academy examinations policy and the additional centre Malpractice Policy.

7. Sharing nudes and semi-nude images

Sexting is defined in our Whole Academy Policy for Safeguarding Incorporating Child Protection which can be found here.
Non-statutory advice from the Department for Education is available to support education settings, this advice can be found here.
This guidance will be used in conjunction with this procedure and Erasmus Darwin Academy's Policy for Safeguarding Incorporating Child Protection.

7.1 Information for Staff responding to concerns regarding nude and semi-nude images

- Staff MUST follow the Safeguarding referral process as outlined in the Safeguarding Policy.
- Concerns related to nude and semi-nude images MUST be reported to the DSL or Deputies.
- Staff MUST NOT ask to see/view any images or videos

7.2 Information for Safeguarding staff responding to concerns regarding nude and semi-nude images

- Speak to the child/children/young person
- Involve parents/carers
- Determine the classification using fig 1 from the DfE Guidance
- Determine if a referral to Social Services or the Police is appropriate NOTE: there is clear guidance in relation to contact with the Police and criminalisation of children in the DfE Guidance.

7.3 Supporting the child/children/ young person

- Establish if the image has been shared
- Ensure the content has been deleted, supervised by a member of staff or parent/carer
- If the image has been shared signpost the child/children/young person to Childline https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/
- Establish if there are wider risks to the child/children/young person and consider a referral to an outside agency as appropriate.

7.4 Role of Parents/Carers

Receive information and advice about the sharing of images

- Support your child/children to delete any inappropriate images, including from backups and cloud based storage.

- Support your child/children with contacting Childline to report and remove shared images https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/
- Be aware of the law in relation to sharing materials
- Support Academy with consent to a referral to external agencies, where appropriate

8. Acceptable use of the internet in the Academy

- All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet). Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.
- Use of the Academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.
- More information is set out in the acceptable user policies

9. Students using mobile devices in the Academy

- Students who require the use of Laptops or other electronic devices must do so in accordance with the Acceptable User Agreement and with the approval of the Senior IT Technician and parents/carers consent.

10. Students using school devices off site

- All students who are loaned an Academy device will have to sign an additional agreement and consent form. Students/Families are liable for costs associated with damage to loaned items.
- Students using Academy devices should be made aware that they are monitored using our monitoring software, inappropriate use could result in pastoral or safeguarding follow up.
- Students using Academy loaned devices should ensure they are not used for purposes other than education or by other members of the household who do not have authorised access to the Erasmus Darwin Academy network.
- Students must not share username and password details with anyone else to prevent unauthorised access to the Erasmus Darwin Academy network.

11. Staff using work devices outside school

- Staff members using a work device outside the Academy must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside the Academy. Any USB devices containing data relating to the Academy must be encrypted.
- If staff have any concerns over the security of their device, they must seek advice from the Senior IT Technician.
- Work devices must be used solely for work activities. Staff should be aware that all laptops and PCs are covered by our monitoring software.

12. How the Academy will respond to issues of misuse

Where a student misuses the Academy's ICT systems or internet, we will follow the procedures set out in the behaviour for learning policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
Where a staff member misuses the Academy's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff

disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
The Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.
Our monitoring software senso alerts the DSL and safeguarding officer to any concerns with a screen captures where a concern is identified. This is then recorded on myconcern if appropriate.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The Staffordshire Children's Board Level 1 Training also highlights the risks around Online Safety.
The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements
The DSL/DDSLs log behaviour and safeguarding issues related to online safety. An incident report log is stored on myconcern.

This procedure will be reviewed annually by the DSL. At every review, the procedure will be shared with the local governing body.

15. Links with other policies

This Online Safety Procedure is linked to our:

- Safeguarding incorporating Child Protection
- Behaviour for Learning Policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable User Policy

Appendix A

APPENDICES - ACCEPTABLE USE AGREEMENTS

Student ICT Acceptable Use Agreement (Years 7-11)

I understand that the internet is not to be used to access or to send to others anything which is illegal, or anything that someone else may find offensive. This would include indecent images, abusive or offensive images and words and items which lead to upset, discrimination, racial or religious hatred. If I am unsure, or if I come across anything which makes me feel uncomfortable, I will turn my computer monitor off and let a teacher know.

I know that I cannot use a mobile phone or other personal digital device on the Academy site for any reason. My phone must be switched off and in my bag while I am on site. I must never access social media sites, messaging, chatrooms or send texts in the Academy day. I must not take photos or record video or make sound recordings with any personal mobile device. If I misuse my phone or other personal device, I know it will be confiscated.

I will always be polite when I use Academy devices or systems. I will never be abusive or use foul language in my on-line communications.

I will treat all Academy ICT equipment with care and respect. I will never harm Academy systems or attempt to access, change or destroy files and systems belonging to the Academy. I will not attempt to access files that I am not entitled to see or use. I will report any problems to a member of staff.

I understand that every person in the Academy has a different computer login and password. I will never allow anyone else to use my details. I will change my password if I think someone else may have my details.

I will not link devices that are themselves computers (this includes mobile phones and tablet devices) to the Academy network unless I am told to do so by the IT Manager.

I will not send or post negative remarks about the Academy or any staff or any students associated with the Academy via phones or other personal devices or via Academy computers, devices or systems. Neither will I send negative messages against the Academy or people within the Academy via the internet, social media sites, blogs or webpages.

I will not take part in ‘cyber-bullying’ by sending or posting humiliating, harmful or cruel images, or setting up blogs or websites or similar communications using the internet or other digital communication devices. This applies both during the Academy day and when I am outside the Academy.

I will not post or send inappropriate pictures or videos of myself or others or upload these onto social networking sites. I will not forward inappropriate pictures that I have received from somebody else as this could be illegal.

I will not open unexpected or suspicious files. I will beware of fake profiles and people pretending to be somebody else. If something doesn’t feel right I will follow my instincts and report it to an appropriate adult. I will never create a false profile as a joke and pretend to be somebody else. I will not spam people or send needless or anonymous messages.

I understand that the Academy will log and monitor my use of computers and devices and my digital communications. I will never try to bypass any of the security in place in the Academy; this includes using proxy bypass sites. This security is in place to protect me from illegal sites, and to prevent hacking into other people’s accounts.

I will not take information from the internet and use it as my own. A lot of information is copyright, which means that somebody else owns it and it is illegal to use this information without permission from the owner. If I am unsure, I will ask an adult. I will not pretend that the work of other students or others outside the Academy is my own – THIS IS PLAGIARISM.

I understand that if I fail to follow these conditions, or if I deliberately misuse Academy ICT, this will result in disciplinary action.

Agreement and Understanding:

By signing this document, the Academy assumes you have read and understood all of the above and that you understand that any of your electronic communications could be looked at if they are related to your well-being, and that you understand that any electronic communications related to the Academy are not entirely private.

Student Signature _____ Date _____

Parent Signature _____ Date _____

Appendix B

ICT Acceptable User Agreement for Students in Sixth Form

I understand that the internet is not to be used to access, display, or to send to others anything which is illegal, or anything that someone else may find offensive. This would include indecent images, abusive or offensive images and words and items which lead to upset, discrimination, racial or religious hatred. If I am unsure, or if I come across anything which makes me feel uncomfortable, I will turn my computer monitor off and let a teacher know.

I know that I cannot use a mobile phone anywhere on the Academy site apart from in the Sixth Form Work Room and Common Room. I must not take photos or record video or make sound recordings with my mobile or any other personal digital device.

If I bring my own device to participate in the 'bring your own device (BYOD)' programme, I will ensure that I use this in a responsible manner within the Academy to enhance my study. I understand that my device must be connected to the Academy WIFI which will provide online access through Academy internet connections which are subject to firewalls, filtering and monitoring for my own safety and that of others within our Academy community.

Personal devices are brought into the Academy entirely at the risk of the owner and the decision to bring the device in to the Academy lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in the Academy

The Academy accepts no responsibility or liability in respect of lost, stolen or damaged devices while at Academy or on activities organised or undertaken by the Academy (the Academy recommends insurance is purchased to cover that device whilst out of the home)

The Academy accepts no responsibility for any malfunction of a device due to changes made to the device while on the Academy network or whilst resolving any connectivity issues

The Academy recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the Academy. Pass-codes or PINs should be set on personal devices to aid security

The Academy is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

If I misuse my phone or any other personal digital devices, I know it will be confiscated.

I will always be polite when I use Academy devices or systems and connections. I will never be abusive or use foul language in my on-line communications.

I will treat all Academy ICT equipment with care and respect. I will never harm Academy systems or attempt to access, change or destroy files and systems belonging to the Academy. I will not attempt to access files that I am not entitled to see or use. I will report any problems to a member of staff.

I understand that every person in the Academy has a different computer login and password. I will never allow anyone else to use my details. I will change my password if I think someone else may have my details.

I will not send or post negative or inappropriate remarks about the Academy or any staff or any students associated with the Academy via phones or other personal devices or via Academy computers, devices or systems. Neither will I send negative messages against the Academy or people within the Academy via the internet, social media sites, blogs or webpages.

I will not take part in 'cyber-bullying' by sending or posting humiliating, harmful or cruel images, or setting up blogs or websites or similar communications using the internet or other digital communication devices. This applies both during the Academy day and when I am outside the Academy.

I will not post or send inappropriate pictures or videos of myself or others or upload these onto social networking sites. I will not forward inappropriate pictures that I have received from somebody else as this could be illegal.

I will not open unexpected or suspicious files. I will beware of fake profiles and people pretending to be somebody else. If something doesn't feel right I will follow my instincts and report it to an appropriate adult. I will never create a false profile as a joke and pretend to be somebody else. I will not spam people or send needless or anonymous messages.

I understand that the Academy will log and monitor my use of computers and devices and my digital communications. I will never try to bypass any of the security in place in the Academy; this includes using proxy bypass sites. This security is in place to protect me from illegal sites, and to prevent hacking into other people's accounts.

I will not take information from the internet and use it as my own. A lot of information is copyright, which means that somebody else owns it and it is illegal to use this information without permission from the owner. If I am unsure, I will ask an adult. I will not pretend that the work of other students or others outside the Academy is my own – THIS IS PLAGIARISM.

I understand that if I fail to follow these conditions, or if I deliberately misuse Academy ICT, this will result in disciplinary action.

Agreement and Understanding:

By signing this document, the Academy assumes you have read and understood all of the above and that you understand that any of your electronic communications could be looked at if they are related to your well-being, and that you understand that any electronic communications related to the Academy are not entirely private.

Student Name _____ Date _____
Student signature_____
Parent Name_____ Date_____
Parent signature_____

Appendix C

Staff ICT Access and Acceptable User Agreement

Erasmus Darwin Academy

The Academy network and associated resources, including SIMS, email and Academy devices including computers, laptops, tablets, Chromebooks, mobile phones, etc are intended for legal activities consistent with the rules of the Academy. All users are required to follow the conditions laid down in the Agreement. Any breach of these conditions may lead to withdrawal of the user's access. Any breach of the conditions may be considered a disciplinary matter and could lead to criminal prosecution.

Conditions of Use

Personal Responsibility

Users are responsible for their own behaviour and communications. Staff are expected to use any ICT resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to the DSL, Deputy Headteacher or Headteacher. Users will note further guidance in the Staff Code of Conduct which gives further detailed information on these matters.

Acceptable Use

Users are expected to utilise the network systems and all Academy ICT hardware in a responsible manner. All Academy computers, devices and systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the Academy ethos, Teachers' Standards and the Safeguarding Policy.

1	I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the academy into disrepute. I will use appropriate language –I will remember that I am a representative of the academy on a global public system. Illegal activities of any kind are strictly forbidden.
2	I will not access, or attempt to access any websites, blogs, social networks that contain any of the following: pornography; promotion of discrimination of any kind; promotion of racial or religious hatred; promotion of obscene or illegal acts; or any other information which may be illegal or offensive to colleagues, students, parents or Governors.
3	I will ensure that all my log-in credentials, including username and passwords are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users. If I think that someone has accessed by password, I will change it immediately and contact the DSL.
4	I will ensure that I log-off after my network session has finished. If I find an unattended machine logged on under another user's credentials, I will <u>not</u> continue using the machine – I will log it off immediately.
5	I will not trespass into other users' files or folders.
6	I will respect the documents and files on the Academy network, and all other linked software as part of the INTELLECTUAL PROPERTY of Erasmus Darwin Academy. Therefore, I will not share any documents or files with other parties without seeking permission from the Headteacher. Neither will I claim ownership of documents and files that have been produced during my employment at Erasmus Darwin Academy.

7	I will not use the Academy ICT systems in any way that would disrupt the network by others. I will not harm or destroy any equipment or data through wilful damage or by uploading or creating viruses that will harm the network. I will report any concerns or problems with the network to the Senior IT technician immediately.
8	I will report any accidental access to or receipt of inappropriate or illegal materials or filtering breaches to the DSL.
9	I will not download any unapproved software, system utilities or resources that may compromise the Academy network or which are not adequately licensed.
10	I will not connect a laptop, tablet, smart phone or other device to the Academy network without permission from the Senior IT technician. The Academy does not accept responsibility for damage to personal ICT devices nor are we able to retrieve corrupted or lost data on personal devices.
11	I will not share or publish information that violates GDPR. I am aware that I have access to confidential personal data on children, staff and families associated with the Academy held on SIMS and in other parts of the network which I may only use in my professional capacity and for conducting Academy business in a secure manner.
12	I will not receive, send or publish material that violates copyright law. I will not use or attempt to use the Academy's ICT facilities to undertake any form of piracy or infringement of copyright provisions whether knowingly or not.
13	I will ensure that portable ICT equipment such as laptops, tablets, digital and video cameras are securely locked away when they are not being used. I will not remove these items from the Academy without permission from the DSL/Senior IT technician. I am not permitted to use any ICT equipment for personal use without written permission from the DSL/Senior IT technician.
14	I will not use personal digital cameras or camera phones to create or transfer images of children or young people without the express permission of the DSL/Headteacher. If permission is granted, images of children and young people associated with the Academy must be uploaded to the network as soon as possible. They must not remain stored on personal devices.
15	I will not accept invitations from any students in the Academy to add me as a 'friend' to their social networking sites, nor will I invite them to be 'friends' on mine. I will follow advice in the Staff Code of Conduct concerning any communication with ex-students.
16	I will ensure that any private social networking sites, chatrooms, messages, blogs, etc that I create or actively contribute to, are not confused with my professional role in any way. I will not engage in any online communications that may compromise my professional responsibilities, and I will ensure that I follow guidance in the Staff Code of Conduct in my online activities.
17	The Academy computer systems cannot be used for ordering personal goods and services.
18	Private or personal chat services, messaging or social networking must not be accessed under any circumstances, at any time of the day, using the Academy computer system.
19	Academy e-mail is for professional communications only. Staff must not use Academy e-mail to send or receive personal messages. I am aware that Academy e-mail communications are not guaranteed to be private.

---------- ✂ ----------

Staff User Agreement Form for the Staff Acceptable Use Agreement

As a user of the network resources, I agree to follow the Academy rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the Academy Acceptable Use Agreement. If I am in any doubt I will consult a member of the Senior Leadership Team.

I agree to report any misuse of the network to DSL, Deputy Headteacher or Headteacher.

I also agree to report any websites that are available on the Academy Internet that contain inappropriate material to DSL/ Senior IT technician.

Lastly I agree to ensure that portable equipment such as laptops, tablets, Chromebooks, mobile phones, etc will be kept secured when not in use and to report any lapses in physical security to the DSL.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name: _____

Staff Signature (if appropriate): _____

Date: _ _ /_ _ /_ _ _ _

Appendix D

Parent ICT Acceptable Use Agreement

The purpose of this Acceptable Use Policy is to protect the security of Academy information and to engender good practice in communications between parents and the Academy. Only parents and guardians authorised by Erasmus Darwin Academy may access Edulink and associated software, eg Wisepay.

Personal Use

Information made available through Edulink is confidential and is protected by law under the Data Protection Act (1998).

- I will not distribute or disclose any information obtained from Edulink to any person(s) with the exception of the student to whom the information relates, or to other adults with parental responsibility for my child.
- I will not attempt to access Edulink in any environment in which the security of the information contained thereon might be placed at risk - e.g. in a public place.

Security

Parents and guardians are responsible for the safety and security of Edulink accounts.

- I will not disclose my usernames and passwords to anyone else nor allow others to access my account.
- I will not access the parent Edulink using anyone else's account.
- I will not share my logon details with my own children.

Copyright

Parents are permitted to view, copy and print documents hosted on the parent Edulink subject to the following conditions:

- I will use the material solely for my own personal information and not for any commercial purpose
- I will not modify the documents or images in any form or manner
- I will not copy or distribute images separately from their accompanying text and will not quote materials out of their context

Communications

Parents are required to ensure that all communications via the Academy network are polite and appropriate at all times. Subject to agreement by the parties concerned, the Academy may give parents and guardians access to staff email addresses:

- I understand that staff email addresses will be used for the sole purpose of communications regarding Erasmus Darwin Academy activities and events, and the education of my own child/children.
- I understand that I have a duty of confidentiality towards the Academy. I will not divulge or communicate to any person or organisation any confidential information relating to or belonging to the Academy.

- I understand that if I fail to comply with this agreement the Academy has the right to remove my access to Academy systems and devices.

Sixth Form Bring Your Own Device

· I understand that students who bring their own device into the Sixth Form must use the Academy WiFi so that appropriate filtering is in place.

· I understand that the Academy advises for children under 18 years of age, parental restrictions are placed on any device to restrict any illegal or inappropriate access to online material and to limit any inappropriate contact.

I agree to comply with the rules and regulations set out in the Erasmus Darwin Academy ICT Acceptable Use Policy Agreement.

Signed: _____

Name: _____

Date: _____

Appendix E

Visitor ICT Acceptable Use Policy Agreement

I understand that I must use the Academy's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.

- I understand that my use of the Academy's systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into Academy for any activity that would be inappropriate in a Academy setting.
- Whilst in the Academy, I will not try to upload, download or access any materials which are illegal (for example 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 programs or software to bypass the Academy's filtering and security systems in order to access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Online Safety Officer.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove, add to or otherwise alter any other user's files, without permission.
- I will not install or attempt to install programs of any type on a Academy device, nor will I try to alter Academy computer settings, unless I have permission to do so.
- I will not disable or cause any damage to Academy equipment or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the Online Safety Officer.

I understand that if I fail to comply with this agreement the Academy has the right to remove my access to Academy systems and devices.

I agree to comply with the rules and regulations set out in the Erasmus Darwin Academy Visitors ICT Acceptable Use Policy Agreement.

Signed: _____

Name: _____

Date: _____

Appendix F

Governor ICT Acceptable Use Policy Agreement

I understand that I must use the Academy's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.

- I understand that my use of the Academy's systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into Academy for any activity that would be inappropriate in an Academy setting.
- Whilst in the Academy, I will not try to upload, download or access any materials which are illegal (for example 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 programs or software to bypass the Academy's filtering and security systems in order to access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the Online Safety Officer.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove, add to or otherwise alter any other user's files, without permission.
- I will not install or attempt to install programs of any type on a Academy device, nor will I try to alter Academy computer settings, unless I have permission to do so.
- I will not disable or cause any damage to Academy equipment or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the Online Safety Officer.

I understand that if I fail to comply with this agreement the Academy has the right to remove my access to Academy systems and devices.

I agree to comply with the rules and regulations set out in the Erasmus Darwin Academy Governor ICT Acceptable Use Policy Agreement.

Signed: _____

Name: _____

Date: _____