ERNULF ACADEMY
Astrea Academy Trust
INSPIRING BEYOND MEASURE

# Online Safety

## POLICY

| | |
|---|---|
| POLICY LEAD | Kimberley Stamford |
| APPROVED BY | Kimberley Stamford |
| DATE OF APPROVAL | September 2023 |
| LAST REVIEWED ON | September 2023 |
| NEXT REVIEW DUE BY | September 2024 |

## Introduction and Aims

This policy aims to:

Set out expectations for all Ernulf Academy community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the Academy gates and regardless of device or platform.

Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare Scholars for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.

Help staff working with scholars to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the scholars in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of Ernulf Academy, supporting the ethos, aims and objectives, and protecting the reputation of Ernulf Academy

Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other policies such as Ernulf Academy Child Protection and Safeguarding Policy, Ernulf Academy Behaviour Policy & Ernulf Academy Anti-Bullying Policy)

## Scope

This policy applies to all members of the Ernulf Academy community (including staff, scholars, volunteers, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their role.

The Education and Inspections Act 2006 empowers the Principal, to such extent as is reasonable, to regulate the behaviour of Scholars when they are off the site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of the Academy, but is linked to membership of the Academy. The Academy, will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of the Academy day.

## Roles & Responsibilities

Ernulf Academy is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, scholars, families and the reputation of Ernulf Academy

We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

This section outlines the roles and responsibilities for online safety of individuals and groups within the Ernulf Academy.

## Principal

Key responsibilities:

- Foster a culture of safeguarding where online safety is part of Ernulf Academy holistic safeguarding approach
- Oversee the activities of the DSL and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the DSL on all online-safety issues which might arise and receive regular updates on Academy issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO (Data Protection Officer), DSL (Designated Safeguard Lead) and LGC to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the Academy implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the need of scholars, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure LGC are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- Ensure the Academy website meets statutory requirements

## Designated Safeguard Lead / Online Safety Lead

Key responsibilities (although the DSL can delegate certain online-safety duties, e.g. to the online safety coordinator, overall responsibility cannot be delegated; this assertion and all quotes below are from Keeping Children Safe in Education 2022):

- "The designated safeguarding lead should take lead responsibility for safeguarding and child
- protection (including online safety)."
- Ensure "An effective approach to online safety [that] empowers an Academy or college to protect and educate the whole Academy or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with the local authority and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns

- Work with the Principal and DPO to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others)
- Receive regular updates in online safety issues and legislation, be aware of local and Academy trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider Academy life
- Promote an awareness and commitment to online safety throughout the Academy community, with a strong focus on parents, who are often appreciative of Academy support in this area, but also including hard-to-reach parents
- Liaise with Academy technical, pastoral, and support staff as appropriate
- Communicate regularly with the wider SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with leadership and ensure staff are aware.
- Ensure the 2021 DfE guidance on Sexual Violence and Harassment is followed throughout the Academy and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff.

## Network Manager / Academy

The Network Manager is responsible for ensuring that (as listed in the 'all staff' section, plus):

- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / data protection officer to ensure that Academy systems and networks reflect Academy policy
- Ensure all stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc)
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online safety related issues that come to their attention in line with Academy policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Monitor the use of Academy technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with Academy policy
- Work with the Principal to ensure the Academy website meets statutory DfE requirements

## All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL) is
- Read Part 1, and Part 5 of Keeping Children Safe in Education 2023
- Read and follow this policy in conjunction with the Academy Safeguarding Policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with Academy procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL if policy does not reflect practice and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all Academy activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in Academy or setting as homework tasks, encourage sensible use, monitor what scholars/Scholars are doing and consider potential dangers and the age appropriateness of websites
- To carefully supervise and guide Scholars when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Prepare and check all online source and resources before using within the classroom
- Encourage Scholars to follow their acceptable use policy, remind them about it and enforce Academy sanctions
- Notify the DSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the Academy hours and site, and on social media, in all aspects upholding the reputation of the Academy and of the professional reputation of all staff.

## Personal Development Lead

Key responsibilities (as listed in the 'all staff' section, plus):

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the Personal Development Calendar. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their scholars' lives."

- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that Scholars face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the Designated Safeguarding Lead and all other staff to ensure an understanding of the issues, approaches and messaging within Personal Development.

## Computer Studies

Key responsibilities (as listed in the 'all staff' section, plus):

- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in Academy to ensure a common and consistent approach, in line with acceptable-use agreements

## Subject / Curriculum Leads

Key responsibilities (as listed in the 'all staff' section, plus):

- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and Scholars alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online safety element

## Data Protection Officer

Key responsibilities (NB – this document is not for general data-protection guidance):

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Ensure general GDPR guidance is understood and followed by all stakeholders.

## Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the DSL as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

## Scholars (to an age-appropriate level)

Key responsibilities:

- Read, understand, sign and adhere to the scholar acceptable use policy and review this annually
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of Academy and realise that the school's acceptable use policies cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at Academy or outside Academy if there are problems

## Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the Internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Academy will therefore take opportunities to help parents understand these issues.

Key responsibilities:

- Read and countersign the scholar AUP) and ensure their children to follow it
- Consult with the Academy if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the Academy staff, volunteers, governors, contractors, Scholars or other parents/carers.

## Community Users

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the Academy in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the Academy staff, volunteers, governors, contractors, Scholars or other parents/carers

## Education and Training

The following subjects have the clearest online safety links:

- Art & Design
- ICT
- Tutor Sessions (Personal Development)

However, as stated above, it is the role of all staff to identify opportunities to thread online safety through all Academy activities, both outside the classroom and within the curriculum.

Equally, all staff should carefully supervise and guide Scholars when engaged in learning activities involving online technology (including, extra-curricular and extended Academy activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Ernulf Academy we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for SEND scholars) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

## Acceptable Usage Policy

- Parents/carers will be required to read through and sign alongside their child's signature, helping to ensure their children understand the rules
- Staff and regular visitors to the Academy have an AUP that they must read through and sign to indicate understanding of the rules.

## Copyright

- Scholars to be taught an appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations- staff to monitor this.
- Scholars are taught, appropriate to their age, to acknowledge the source of information used and to respect copyright when using material accessed on the Internet.
- If using a search engine for images – staff / children should open the selected image and go to it's website to check for copyright.

## Staff Training

- Online Safety Lead ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- A planned programme of online safety training is available to all staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the Academy Online Safety policy, Acceptable Usage and Child Protection Policies.
- The Online Safety Lead will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released.
- LCG representatives are invited to take part in online safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, online safety, health and safety or child protection.

## Communication

Email:

- Digital communications with scholars (e-mail, online chat, VLE, voice etc.) should be on a professional level and only carried out using official Academy systems.
- The school's e-mail service should be accessed via the provided web-based interface by default (this is how it is set up for the laptops, Academy curriculum systems);
- Under no circumstances should staff contact scholars, parents/carers or conduct any Academy business using personal e-mail addresses. If this happens by mistake, the DSL/Principal/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Academy e-mail is not to be used for personal use. Staff can use their own email in Academy (before, after Academy and during lunchtimes when not working with children) – but not for contact with parents/ scholars.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the Academy into disrepute or compromise the professionalism of staff.

## Mobile Phones

- Academy mobile phones only should be used to contact parents/carers/scholars when on Academy business with scholars off site. Staff should not use personal mobile devices.
- Staff should not be using personal mobile phones in Academy during working hours when in contact with children.
- Scholars should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

## Social Networking Sites

Many social media platforms have a minimum age of 13, but the Academy regularly deals with issues arising on social media with scholars under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years

- Scholars will not be allowed to access social media/ networking sites at school.
- Staff should not access social networking sites on Academy equipment in Academy or at home. Staff should access sites using personal equipment.
- Staff users should not reveal names of staff, scholars, parents/carers or any other member of the Academy community on any social networking site or blog.
- Scholars/Parents/carers should be aware the Academy will investigate misuse of social networking if it impacts on the well-being of other scholars or stakeholders.
- If inappropriate comments are placed on social networking sites about the Academy or Academy staff then advice would be sought from the relevant agencies, including the police if necessary.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the Academy complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, scholars and parents, also undermining staff morale and the reputation of the Academy (which is important for the scholars we serve).

Scholars are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Scholars are discouraged from 'following' staff, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). In the reverse situation, however, staff must not follow such public scholar accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Principal, and should be declared upon entry of the scholar or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Principal (if by a staff member).

Staff are reminded that they are obliged not to bring the Academy or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the Academy or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the Academy into disrepute.

The Academy has an active website and twitter account which are used to inform and publicise Academy events as well as to celebrate and share the achievement of scholars.

## Digital Images

The Academy record of parental permissions granted/not granted must be adhered to when taking images of our scholars.

Permissions are sought for:

- displays around the school
- the newsletter
- use in paper-based Academy marketing
- online prospectus or websites
- a specific high-profile image for display or publication
- social media

Under no circumstances should images be taken using privately owned equipment without the express permission of the Principal.

Where permission is granted the images should be transferred to Academy storage systems (server or disc) and deleted from privately owned equipment at the earliest opportunity. Images are stored on the Academy network in line with the retention schedule of the Academy Data Protection Policy.

Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose

Any scholars shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them)

Although many of the above points are preventative and safeguarding measures, it should be noted that the Academy will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information.

We encourage young people to think about their online reputation and digital footprint. Scholars are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.

Scholars are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

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

## Removable Data Storage Devices

- Only encrypted USB devices are allowed write access. If not encrypted read access only.
- All files downloaded from the Internet, received via e-mail or provided on removable media (e.g. CD, DVD, USB flash drive, memory cards etc.) must be checked for viruses using Academy provided anti-virus software before being run, opened or copied/moved on to local/network hard disks.
- Scholars should not bring their own removable data storage devices into Academy unless asked to do so by a member of staff.

## Websites

- In lessons where Internet use is pre-planned, scholars should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches.
- Staff will preview any recommended sites before use.
- “Open” searches (e.g. “find images/ information on...”) are discouraged when working with younger scholars who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff. Parents will be advised to supervise any further research.
- All users must observe copyright of materials published on the Internet.
- Teachers will carry out a risk assessment regarding which scholars are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the scholars on the internet by the member of staff setting the task. All staff are aware that if they pass scholars working on the internet that they have a role in checking what is being viewed. Scholars are also aware that all internet use at Academy is tracked and logged.
- The Academy only allows the Online Safety Co-ordinator, Network Manager and SLT to access to Internet logs

## Passwords

Staff:

- Passwords or encryption keys should not be recorded on paper or in an unprotected file
- Passwords should be changed at least every 3 months
- Users should not use the same password on multiple systems or attempt to “synchronise” passwords across systems

## Scholars

- Should only let Academy staff know their in-Academy passwords.

- Inform staff immediately if passwords are traced or forgotten. All staff are able to access the network to allow scholars to change passwords

## Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Principal or Network Manager.
- Scholars should not bring in their own equipment unless asked to do so by a member of staff.

## Use of Academy Equipment

- No personally owned applications or software packages should be installed on to Academy ICT equipment;
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs. If it is necessary to do so, the local drive must be encrypted.
- All users should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

## Monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

All use of the school's Internet access is logged and the logs are randomly but regularly monitored by the school's external provider. Whenever any inappropriate use is detected it will be followed up by the Online Safety Lead, Scholar Managers, Progress Leaders or members of the Senior Leadership Team depending on the severity of the incident.

- Online Safety Lead and Network Manager will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems
- Any member of staff employed by the Academy who comes across an online safety issue does not investigate any further but immediately reports it to the Online Safety Lead and impounds the equipment. This is part of the Academy safeguarding protocol. (If the concern involves the Online Safety Lead then the member of staff should report the issue to the Principal).

## Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Principal and staff authorised by them have a statutory power to search scholars/property on Academy premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. All searches must be recorded using the Academy 'Conducting a search' documents and then handed to the Principal and uploaded to CPOMS.

## Incident Reporting

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/PD/RSHE and Citizenship.

Any online safety incidents must immediately be reported to the Principal (if a member of staff - unless the concern is about the Principal in which case the compliant is referred to Astrea Trust Senior Safeguarding Manager and Assistant CEO as per the Ernulf Academy Safeguarding Policy 2023)

Any online safety incidents regarding scholars should be reported on CPOMS.

The Academy will actively seek support from other agencies as needed (i.e. the local authority, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or scholars engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

## Sexting

It is important that everyone understands that whilst sexting is illegal, scholars/scholars can come and talk to members of staff if they have made a mistake or had a problem in this area. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

## Responding to incidents of misuse

It is hoped that all members of the Academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse.

Listed in Appendix 2 are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted.

Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the Academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows (Appendix 3 for scholars and Appendix 4 for staff respectively).

# Appendix 1

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Academy currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

| | Staff and other adults | | | | Scholars | | | |
|---|---|---|---|---|---|---|---|---|
| Communication Technologies | Permitted | Permitted at certain times | Permitted for named staff | Not permitted | Permitted | Permitted at certain times | Permitted with staff permission | Not permitted |
| Mobile Phones may be brought into the Academy | X | | | | X | | | |
| Mobile phones can be used in lessons | | | X | | | | | X |
| Use of mobile phones in social times | X | | | | | | | X |
| Taking photographs on a mobile devices | | | | X | | | | X |
| Use of PDAs and other educational mobile devices | X | | | | X | | | |
| Use of School email for personal emails | | | | X | | | | X |
| Social use of chat rooms / facilities | | | | X | | | | X |
| Use of social networking sites | | | X | | | | | X |
| Use of educational blogs | X | | | | X | | | |

When using communication technologies, the Academy considers the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored. Staff and scholars should therefore use only the Academy email service to communicate with others when in school, or on Academy systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person (in accordance with the Academy policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and scholars or parents/carers (email, chat, Learning Platform etc) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Scholars should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff.

# Appendix 2

Unsuitable / inappropriate activities:

| User Actions | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|
| Child sexual abuse images | | | | | |
| Promotion or conduct of illegal acts eg. Under the child protection, obscenity, computer misuse and fraud legislation | | | | | |
| Adult material that potentially breaches the obscene publications Act in the UK | | | | | |
| Criminally racist material in the UK | | | | | |
| Pornography | | | | | |
| Promotion of any kind of discrimination | | | | | |
| Promotion of racial or religious hatred | | | | | |
| Threatening behaviour, including the promotion or physical violence or mental harm | | | | | |
| Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the Academy or brings the Academy into disrepute | | | | | |
| Using the Academy systems to run a private business | | | | | |
| Uses systems, applications, websites or mechanism that bypass the filtering or other safeguards employed by the Academy Trust. | | | | | |
| Uploading / downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions | | | | | |
| Revealing or publicising confidential or proprietary information | | | | | |
| Creating or propagating computer viruses or other harmful files | | | | | |
| Carrying out sustained or instantaneous high volume network traffic. | | | | | |
| On-line gaming (educational) | | | | | |
| On-line gaming (no-educational) | | | | | |
| On-line gambling | | | | | |
| On-line shopping / commerce | | | | | |
| File sharing | | | | | |
| Use of social media sites | | | | | |
| Downloading video broadcasting | | | | | |
| Uploading to video broadcasting | | | | | |

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from Academy and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a Academy context, either because of the age of the users or the nature of those activities. The Academy believes that the activities referred to in the following section would be inappropriate in a Academy context and that users, as defined below, should not engage in these activities in Academy or outside Academy when using Academy equipment or systems. The Academy policy restricts certain internet usage as follows. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

# Appendix 3

| Incident | Behaviour Policy to be used | CPOMS Log | Refer to Police | Referral to IT Tech support for action re; security / filtering |
|---|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal | | X | X | X |
| Unauthorised use of non-educational sites during lessons | X | | | X |
| Unauthorised use of mobile phone / camera / other handheld devices | X | | | |
| Unauthorised use of social networking / instant messaging / personal email | X | | | X |
| Unauthorised downloading or uploading of files | | X | | X |
| Allowing others to access Academy network by sharing username and passwords | | X | | X |
| Attempting to access or accessing the Academy network by using another Scholarss account | | X | | X |
| Attempting to access or accessing the Academy network using the account of a staff member | | X | | X |
| Corrupting or destroying the data of other users | | X | | X |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | | X | | X |
| Continued infringements of the above, following previous warning or sanctions. | | X | X | X |
| Actions which could bring the Academy into disrepute or breach the integrity of the ethos of the Academy | | X | | X |
| Using proxy sites or other means to subvert the Academy's filtering system | | X | | X |
| Accidentally accessing offensive or pornographic material and failing to report the incident | | X | | X |

The guidance in this policy should be implemented with cross reference to the School's Child Protection, Anti-Bullying and Behaviour Policies.

NB: attempts have been made to synchronise guidance and sanctions.

# Appendix 4

| Incidents involving members of staff | Refer to the Principal. In the event of the breaches of policy by the Principal, refer to the Chair of LGC | Refer to action needed for action regarding filtering and security | Refer to SCC LADO<br><br>Potential Disciplinary Action |
|---|---|---|---|
| Deliberately accessing or trying to access material that could be considered illegal | X | X | X |
| Receipt of transition of material that infringes the copyright of another person or infringes the Data Protection Act | X | | X |
| Excessive or inappropriate personal use of the internet/social networking sites/instant messaging/personal email | X | X | X |
| Unauthorised downloading or uploading of files | X | X | X |
| Allowing others to access Academy network by sharing username and passwords or attempting to access or accessing the Academy network, using another person's account | X | X | X |
| Careless use of personal data | X | | X |
| Diliberate actions to breach data protection or network security rules | X | X | X |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software | X | X | X |
| Sending an email, text or instant message that it regarded as offensive, harassment or of a bullying nature | X | X | X |
| Using a personal email/social networking/instant messaging/text messaging to carry out digital communications with scholars | X | X | X |
| Actions that could compromise a staff members professional standing | X | | X |
| Actions that could bring the Academy into disrepute or breach the integrity of the ethos of the Academy | X | | X |
| Using Proxy sites or other means to subvert the Academy filtering system | X | X | X |
| Deliberately accessing or trying to access offensive or pornographic material | X | X | X |
| Breaching copyright or licensing regulations | X | X | X |
| Continued infringements of the above, following previous warning or sanctions. | X | | X |

# Appendix 5

## Acceptable Usage Policy – Scholars

KS3/4 Acceptable Use Agreement

What is an AUA?

We ask all young people and adults involved in the life of Ernulf Academy to sign an Acceptable Use Agreement, which is a document that outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

Why do we need an AUA?
These rules have been written to help keep everyone safe and happy when they are online or using technology. Sometimes things go wrong and people get upset, but these rules help us avoid it where we can.
School systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. This means anything you do on a school device or using school networks/platforms/internet (including from home when home learning) may be viewed by one of the staff members who are here to keep you safe.
But it's not about systems and devices – it's about behaviour. So the same rules apply when you are at school as when you are home learning or just having fun with friends.

Where can I find out more?

If your parents/carers want to find out more, they can read Ernulf Academy's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUA, please speak to Mrs Kimberley Stamford, Designated Safeguarding Lead

What am I agreeing to?

BEHAVIOUR - FOR ANY DEVICE, APP, SITE OR GAME, AT SCHOOL AND AT HOME:

- Anything I write, post or share online will be necessary, relevant, positive and respectful.
- I will treat myself and others with respect at all times, treating others the way I would like to be treated and speaking to people as I would face to face.
- I will always be positive and creative, aiming to learn and share, develop new skills, have fun and prepare for the future.
- I know it can be hard to put down devices (for adults too), so when parents/carers or teachers talk to me about it, I will be open and honest if I am struggling.
- I will always protect my reputation and that of the school, staff, scholars and others.

- I only use apps, sites and games I am old enough for. I know most social media are 13+ and games can have higher age ratings. I know 18-rated games are not just more difficult but are only suitable for people over this age. They could be harmful to me if I am under 18.

- When I am at school or using a school system or device, I will only use apps, sites or games that I have been told are appropriate for school use.

- I will always avoid taking risks online and doing anything that encourages hate, discrimination or bullying.

- I know just calling something banter doesn't make it okay - if it is upsetting it could become bullying; if jokes are all one-sided, and the other person is upset, it is time to stop!

- I will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside. I will stand up for my friends by sharing this with a Trusted adult.

- I know people online might not be who they say they are, even if the picture and name are from someone I know, so I am always very careful when someone wants to add me.

- I will always talk to a trusted adult before I meet someone face to face who I have only met online. I will never meet anyone I meet online alone.

- I will only use my personal devices (mobiles, smartwatches etc) in school if I have been given permission, and I will never take secret photos, videos or recordings of teachers or scholars, including when learning remotely.

- I will check location and privacy settings the first time I install an app and regularly afterwards because many apps can show everyone where I am, where I live and go to school (I know that they may reset without asking).

- I don't have to keep a secret or do a dare or challenge just because someone (even a friend) tells me to – real friends don't put you under pressure to do things you don't want to. If I promise to do something and then realise it is a bad idea, I don't have to do it.

- I can always say no online, end a chat or block someone.

- I will not attempt to watch pornography on a school device. I know that there are risks associated with watching pornography online. Children and young people who watch porn or sexually explicit content are at greater risk of developing:

I. unrealistic attitudes about sex and consent

II. more negative attitudes about roles and identities in relationships

III. unrealistic expectations of body image and performance

- I will treat all devices with respect. I will not cause any physical damage, or try to change something, that could cause difficulty for someone else. If I use a device and find that it has been damaged, or something has been changed, then I will tell a trusted adult immediately. If I damage a device on purpose, I understand that I will be subject to the Academy's behaviour policy and any applicable sanctions.

SHARING:

- I know anything I do can be shared and may stay online forever - even disappearing or anonymous messages can be traced and saved; deleting a post won't remove people's screenshots. Anything I do online now may be available online when I am an adult and poor decisions could affect my future.

- I will respect my body and other people's: use positive language; not share photos or videos to shame or embarrass; never share revealing images or where I/they aren't fully dressed.

- It is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying; I will not share or forward it, but I will ask a trusted adult for advice/help.

- I will not post, look at, upload/download or share material that could be offensive, misleading, harmful or illegal. If I come across anything that is of concern, I will report it immediately.

- I will not share anybody's personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission or reviewed the site.

- I will always check sources before sharing news or information, because I know anything I see online could be biased and misleading, and there are lots of spoof accounts.

- If I choose to Livestream, I will make sure my parents/carers know about it first, and I will always check my privacy settings and know who can see what and when. I am careful what information I share during at Livestream, and make sure that I do not say things that could upset or hurt others.

ACCESS, SECURITY & SETTINGS:

- I understand that the school may be able to track my activity whenever I am on any school device or system, including school devices or systems when I am at home. This means they may be able to access my emails or see what websites I visited. School computers, laptops and devices are monitored, and anything that I type or view while using these devices can be seen by Teachers and Staff at School.

- I will keep login details secret and change my password regularly. If I think someone knows my password, I will change it; if I think they have used it, I will tell a teacher.

- I will not try to bypass school security in any way or access any hacking files or tools.

- I will only edit or delete my own files and not view, change or delete other people's files or user areas without their permission.

- If I am not expecting to receive a file or link from someone, or it looks strange to me, I will double-check with the person it is from (in a new message, not by clicking reply) before clicking.

- I will not download copyright-protected material (text, music, video etc.).

- I understand that internet access in School is filtered to reduce the likelihood of unsuitable material being shown on School devices, but I know that I can report anything that I think should be filtered to a trusted adult.

GETTING HELP:

- I will tell a trusted adult if I have a problem or am worried about something online, and I will encourage my friends to do so too. Even though it might not feel like it, statistics show that telling someone helps!

- If I see anything that shows people self-harming or encouraging others to do so, I will report it on the app, site or game and tell a trusted adult straight away.

- School staff and private tutors should not behave differently in private or online than when the whole class is in a room together, so if I ever get asked or told anything online that would be strange in school, I will tell another teacher.

- I might be contacted online on Bromcom, Office 365, Email or Microsoft Teams by my teachers, school staff or tutors about my learning, wellbeing or behaviour. If I am contacted by someone else, I will tell another teacher.

- If I see, watch, read, hear or receive anything I am unhappy with or I receive a message that makes me feel uncomfortable, e.g. bullying, sexual, violent or extremist/hateful content, I will not respond to it but I will talk to a trusted adult about it.

I know I can also report unwanted sexual harassment or abuse from the school community and get help form the Designated Safeguarding Lead, Mrs Kimberley Stamford or via the NSPCC at help@nspcc.org.uk or by calling 0800 136 663.

- I know who my trusted adults are at school, home and elsewhere, but I can also get in touch with Childline, The Mix, or The Samaritans. You can also email staysafe@astreaernulf.org

## Appendix 6

### Staff E-safety & Staff Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in Academy. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Executive Principal.

- I will only use the Academy's system, email and internet for professional purposes.
- I will comply with the ICT system security and not disclose any passwords provided to me by the Academy.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any Academy business.
- I will ensure that personal data is kept secure and is used appropriately.
- I will not use or install any software without permission from the IT team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with Academy policy and with written consent of the parent, carer or staff member.
- Images will not be distributed outside the Academy network without the permission of the parent/ carer, member of staff or Executive Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Executive Principal.

- I will ensure that my online activity, both in the Academy and outside the Academy, will not bring my professional role into disrepute.
- I will support and promote the Academy's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

I agree to follow this code of conduct and to support the safe use of ICT throughout the Academy.

Please sign and return to the School Business Manager

Name……..

Signature ……

Date ……..