Doucecroft School Services

E-Safety Policy

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of document</td>
<td>Final</td>
</tr>
<tr>
<td>Version</td>
<td>3</td>
</tr>
<tr>
<td>Date ratified</td>
<td>12th September 2017</td>
</tr>
<tr>
<td>Ratified by</td>
<td>Clive Stobbs</td>
</tr>
<tr>
<td>Release date</td>
<td>September 2017</td>
</tr>
<tr>
<td>Review date</td>
<td>September 2019</td>
</tr>
<tr>
<td>Document owner</td>
<td>Human Resources</td>
</tr>
<tr>
<td>Document Authors</td>
<td>Dan McCullagh, Sam Lawrence, Kuben Reddy, Hayley Greenhill</td>
</tr>
</tbody>
</table>
Contents

1 Introduction ........................................................................................................................................ 3
  1.1 Technology ...................................................................................................................................... 4
  1.2 What is e-safety? ............................................................................................................................. 4
  1.3 The risks .......................................................................................................................................... 4
  1.4 Objectives of this Policy .................................................................................................................. 5
  1.5 Policy Impact ................................................................................................................................... 5
  1.6 Scope of this Policy .......................................................................................................................... 6
  1.7 Terminology .................................................................................................................................... 6

2 Implementation and Responsibilities ..................................................................................................... 7
  2.1 Trustees .......................................................................................................................................... 7
  2.2 Governors ...................................................................................................................................... 7
  2.3 Chief Executive ............................................................................................................................... 7
  2.4 Head Teacher, Directors and Senior Managers .............................................................................. 7
  2.5 IT Manager ..................................................................................................................................... 7
  2.6 E-Safety Co-ordinators/Champions ................................................................................................. 8
  2.7 Designated Persons for Safeguarding .............................................................................................. 8
  2.8 Staff Supervising Individuals Online .............................................................................................. 9
  2.9 All Staff ......................................................................................................................................... 9
  2.10 Students and Service Users .......................................................................................................... 9
  2.11 Parents and Carers ......................................................................................................................... 9

3 Maintaining E-Safety .......................................................................................................................... 10
  3.1 What Constitutes an E-Safety Incident? ......................................................................................... 10

4 Preventing E-Safety Incidents ............................................................................................................... 11

5 What to Do If You Are Involved in an E-Safety Incident ................................................................. 12
  5.1 Reporting an E-Safety Incident ....................................................................................................... 12
  5.2 Staff reporting an E-safety Incident involving a Student or Service User ...................................... 12
  5.3 How Students and Service Users can Report an E-Safety Incident .............................................. 13
  5.4 Reporting Other Members of Staff Involved in an E-Safety Incident ............................................ 13
  5.5 In Each Case .................................................................................................................................. 13
  5.6 What Happens Next? ..................................................................................................................... 13
    5.6.1 If there has been inappropriate communication or contact .................................................. 13
    5.6.2 If someone has been bullied .................................................................................................... 14
    5.6.3 If someone has received malicious/threatening comments .................................................. 14
    5.6.4 If an illegal website has been viewed (see Section 5.7 below) .............................................. 14
    5.6.5 If an inappropriate website has been viewed (see Section 5.7 below) .................................. 15
  5.7 Is a site Illegal or Inappropriate? ................................................................................................... 15

6 Support and Sanctions Following an Incident ....................................................................................... 16

7 Acceptable Use Agreements ................................................................................................................ 17

8 Other Resources .................................................................................................................................. 18

9 Appendix 1 – Contact Information ..................................................................................................... 19
Doucecroft School Services are part of Autism Anglia’s services to people with autism. As part of this organisation, the school has adopted this policy to support staff performance during the school day and within its residential services.
1 Introduction

1.1 Technology

New technologies have become integral to our lives in today's society, within school, work and in our personal lives. The internet and other digital information and communication technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning.

1.2 What is e-safety?

E-safety is defined as being safe from risks to personal safety and wellbeing when using any fixed or mobile device that allows access to the internet or communicates electronically by other means. This includes personal computers, laptops, iPads and other tablets, mobile phones and gaming consoles such as Xbox, Playstation and Wii.

Safeguarding against these risks is everyone's responsibility, not just for those within ICT, and needs to be considered as part of the arrangements that safeguard and promote the welfare of all members of the community, in particular the vulnerable.

1.3 The risks

Those with individuals in their care should be mindful of specific safeguarding. The following risk areas have elements which could or are likely to include occur online:

- Child Sexual Exploitation
- Exploitation of Vulnerable Adults
- Bullying, including cyberbullying
- Faith abuse
- Radicalisation
- Sexting
- Teenage relationship abuse
- Trafficking

These are some of the more specific risks and dangers that people may face when using an online device:

- Access to illegal, harmful or inappropriate images, videos, games and other content
- Unauthorised access to / loss of / sharing of personal information (including personal details, images, videos etc.)
- The risk of being subject to grooming by those with whom they make contact on the internet
- Cyber-bullying and Trolling
- Inappropriate communication or contact with other internet users, including strangers
- The publication or communication of material or language which other internet users may find offensive or harmful
- Sharing / distributing another person's personal information (including personal details, images, videos etc.) without the individual's knowledge or consent
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
• Illegal downloading of music or video files
• The transmission or receipt of computer viruses
• The potential for excessive use which may impact on the social, emotional, development and learning aspects of life

Many of these risks reflect situations in other aspects of life and it is essential that this e-safety policy is read in conjunction with other relevant policies and documents. It should also be noted that many children and adults with an autism spectrum condition could have increased levels of vulnerability to being affected by or drawn into many of these online risks.

It is impossible to eliminate those risks completely. It is therefore essential, through improving awareness and good educational provision, to build resilience to the risks to which our staff and the children and adults we work with may be exposed, so that we all have the confidence and skills to face and deal with those risks.

1.4 Objectives of this Policy

Internet Access is provided at our establishments to enable those in our care to lead normal lives, to raise educational standards, promote achievement, support the professional work of staff and enhance management functions.

It is the duty of all organisations which provide any form of learning to foster a safe and welcoming environment. It is important to teach all our staff and all those we support the necessary skills to use the internet appropriately, to know and understand the associated risks and to allow them to take care of their own safety and security.

We do understand that some people are naturally inclined to better understand and make use of the various devices used to communicate over the internet and we make it a priority that suitable training is offered to any staff members who are expected to use email and/or the internet as part of their job role. Particular emphasis for training will be given to those who use these services while supervising an adult or child we support.

Staff, students and service users will be taught about acceptable use of Autism Anglia’s internet and ICT facilities and given clear expectations for internet use. Where appropriate, staff, students and service users will be made fully aware of the consequences of any breaches to these expectations. As an organisation, we need to strike an effective balance between education to take a responsible approach and the use of regulation and punishment. Responses to breaches of this policy should be considered on a case by case basis, taking into account the nature of the event and the role of the individuals within the organisation.

The organisation will work with relevant groups to ensure that the systems to protect students and service users are reviewed and improved upon, and this will depend on an effective system of reporting any misuse or gaps in our protection systems.

E-safety depends on everyone from governors and trustees to staff, parents and the students/service users themselves playing their part in this policy. Staff have a responsibility to supervise those in our care, to plan their access and to be an appropriate role model.

1.5 Policy Impact

The report following an Ofsted inspection at Doucecroft in 2014 stated:

“All staff and students receive training in e-safety and show a clear understanding of the dangers of inappropriate use of social media. The school recognises that issues often originate out of school and involves parents and carers by sending them its e-safety policy. Students understand risk and are able to respond appropriately. One student received messages on a social media site encouraging him to become involved with an extremist organisation. The school had prepared him well; he was able to identify the nature of the approach and reject it.”
1.6 Scope of this Policy

This policy sets out clear guidelines for ensuring all our staff and those we support remain safe when using the internet and other methods of communication.

This policy affects all staff, volunteers, service users and students:

- while on an Autism Anglia site
- while representing Autism Anglia to other individuals or in another location
- while overseeing or permitting another member of the Autism Anglia community to use a device capable of communicating electronically, either over the internet or via other methods
- while accessing or using Autism Anglia’s networks and/or data remotely (i.e. from 'off-site')
- while communicating with or about any member of the Autism Anglia community

For Service Users within our Adult Services, this policy does not affect:

- their right to privacy while in their own room or
- their right to make their own decisions

However, it is expected that with appropriate education, they will be able to make safe and informed decisions about their internet use. Note that this exception does not apply to staff in sleep-in rooms.

All Autism Anglia staff, students and service users have rights and responsibilities under this policy.

1.7 Terminology

“The Organisation” means Autism Anglia, including Head Office, Dereham Office, School Services and Adult Services.

“Staff” or “staff member” means any person working for, volunteering with, contracted to or sub-contracted to the organisation.

“Service Users” refers to individuals who receive direct support through the organisation’s Adult Services, including Residential Care, Support Living and the Adult Study Centres.

“Adult we support” refers to anyone aged 18 or over receiving a service from Autism Anglia, including Adult Services, School Services, Family Support and other services (e.g., work experience).

“Student” refers to any child attending Doucecroft School or the FE Department, or receiving another service on-site, e.g. respite care.

“Child we support” refers to anyone up to the age of 18 receiving a service from Autism Anglia, including School Services, Family Support and other services.

“School Services” refers to Doucecroft School.

“IT” means Information Technology. “ICT” means Information Communication Technology. These terms are used interchangeably.

The “Autism Anglia Community” refers to anyone with direct contact with Autism Anglia on a day to day basis, including staff, volunteers, students and service users.
2 Implementation and Responsibilities

2.1 Trustees
It is the role of the Trustees to define Autism Anglia’s policy in respect of online safety, taking into account the legal and stakeholder requirements. The Trustees are also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

2.2 Governors
Approving the E-safety policy for use within Doucecroft School and reviewing its effectiveness.

2.3 Chief Executive
The Chief Executive is the named officer with responsibility for ensuring that the Autism Anglia complies with its statutory obligations.

2.4 Head Teacher, Directors and Senior Managers
Ensuring the safety of all members of the Autism Anglia community.
Ensuring adequate Continual Professional Development is provided around E-safety.
Following procedures in the event of a serious e-safety allegation being made against or concerning a member of staff, a student or a service user within Autism Anglia.

2.5 IT Manager
The Information Technology Manager has responsibility delegated from the Chief Executive for ensuring that effective systems and processes are in place to address e-safety.

This person is responsible for:

- Taking a lead role in day to day E-safety issues.
- Reviewing the E-safety policy according to its schedule.
- Ensuring that E-safety is included in the school’s 3 year plans.
- Log all E-safety incidents to help inform future E-safety practices / developments.
- Attend relevant meetings where appropriate.
- Report to Senior Management when necessary.
- Oversight of E-Safety Co-ordinators/Champions and convening regular team meetings.

In addition, the IT Manager will ensure that:

- The organisation’s computer network infrastructure is secure and not open to misuse or attack.
- Emerging technologies are examined for potential benefits and a risk assessment is carried out before their use is permitted.
- Autism Anglia remains up to date with e-safety technical information, sharing best practice with others as necessary.
- All staff are aware of the issues and attend training on at least a 2-yearly basis.
- Where web filtering is present, it is kept up to date and monitored.
- At smaller sites, appropriate measures are in place to monitor internet use.
- Ensuring data is held in line with the Data Protection Act 1998.
- Virus protection is installed and updated regularly.
- Files held on the organisation’s networks are regularly checked.
2.6 E-Safety Co-ordinators/Champions
Within our various services, the E-Safety Co-ordinators and E-Safety Champions will support the IT Manager by:

- Taking a lead in day to day e-safety issues in their service.
- Assisting staff, service users and students in their service with e-safety education, training and support.
- Having an up to date awareness of E-safety matters by attending staff training and regular team meetings.
- Monitoring internet access and logging any issues at their service (where applicable).
- Receiving e-safety incident reports and processing or forwarding them as appropriate.
- Feeding back comments, trends and observations to the IT Manager.

2.7 Designated Persons for Safeguarding
Within our various services, the Designated Persons for Safeguarding are also responsible for:

- Having an up to date awareness of E-safety matters.
- Having an up to date awareness of the potential risk for serious safeguarding issues such as:
  - sharing of personal data
  - access to illegal/inappropriate materials
  - inappropriate contact with strangers
  - sexual exploitation (child and vulnerable adult)
  - potential/actual grooming
  - cyberbullying
- Be aware of the routes for reporting E-safety incidents (e.g. police, click CEOP)

At the time of writing, the Designated Persons for Safeguarding are:

- Doucecroft School Head Teacher
- Doucecroft School Assistant Head Teachers
- Doucecroft School Care Manager
- Doucecroft School Behaviour Support Manager
- Doucecroft School Deputy Care Manager
- Doucecroft School Head of Further Education
- Director of Adult Services
- Adult Services Registered Service Managers

Our Designated Persons for Safeguarding are overseen by the Deputy Chief Executive and by a member of the board of trustees who has responsibility for Safeguarding.

These positions are listed again in Appendix 1, with current post-holders and contact information.
2.8 **Staff Supervising Individuals Online**

When staff are using or overseeing the use of the internet or other communication methods, it is vital that all staff:

- Understand the risks involved when using the internet
- Understand additional risks when allowing people in our care to use the internet
- Remain diligent when using the internet at work
- Maintain appropriate oversight of those we support while they are using the internet
- Remain up to date with relevant policies, management plans, risk assessments, support plans, care plans and education plans which may affect the way those we support use the internet.

2.9 **All Staff**

All staff working for Autism Anglia are responsible for:

- Having an up to date awareness of E-safety matters, including this policy. All staff should attend E-Safety training on a 2-yearly basis, and read additional material supplied by the E-Safety Team.
- Familiarising themselves with the organisation’s Confidentiality and Data Protection Policy and the IT, Internet and E-mail Policy.
- Reporting any suspected misuse to the E-safety co-ordinator/champion and/or a designated person for safeguarding for investigation, sanction and/or support.
- Ensuring all digital communication, including email, mobile phone text with students or service users is on a professional level and only carried out using Autism Anglia systems.
- Ensuring other staff, students and service users are aware of the relevant policies and that any breaches are reported through the relevant procedures.
- Ensuring that copyright law is abided by when using materials from the internet.
- Being aware that Internet traffic can be monitored and traced to individual users. Discretion and professional conduct is essential.

2.10 **Students and Service Users**

When using our ICT systems, our Students and Service Users agree to:

- Ensure they use our ICT systems appropriately, following guidelines and policies.
- Report issues of abuse/misuse within the organisation and know how to do so.
- Know and follow organisation and/or school policy on the use of mobile phones and digital cameras
- Observe the guidelines laid out in the IT, Internet and Email Policy and the Data Protection and Confidentiality Policy which govern the appropriate use of information including images and videos.
- Understand the importance of good e-safety practice when using digital technology.
- Ensure copyright is observed when using information from the internet.

2.11 **Parents and Carers**

We ask that parents and carers make themselves aware of the risks surrounding people using the internet, and endorse the areas of this policy which govern those in their care. Autism Anglia will offer practical guidance to families of our students and service users in the form of sessions for parents and information via various methods, e.g. leaflets, web site, emails, etc.
3 Maintaining E-Safety

All people have the right to be and to feel safe when using the internet and other digital communication technologies. There are many risks prevalent in today's society, including abuse, violence, racism and exploitation, from which we all need to protect ourselves and those around us.

This is even more important given the vulnerable nature of many of the adults and children we support.

It is also understood that for many people with autism, the internet may appear to be a safer, more understandable place. For example, there is no requirement to understand many of the complexities involved in talking to someone face to face, from tone of voice to facial expressions and body language. As an organisation, we should be encouraging our students and service users to use the internet an appropriate amount, to maintain a balance with other social activities.

Staff, students and service users need to be aware of what constitutes inappropriate material, situations and internet use, and of how to cope and what to do if they come across any of them.

3.1 What Constitutes an E-Safety Incident?

This list refers to the examples in Section 1.3 of this document which has been duplicated here for easy reference. This is not intended as an exhaustive list as other material, circumstances or behaviour could easily fit into this list.

- Access to illegal, harmful or inappropriate images, videos, games and other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- Cyber-bullying and trolling
- Inappropriate communication, content or contact with other internet users, including strangers
- The publication or communication of material or language which other internet users may find offensive or harmful
- Sharing / distributing personal information (including images, videos etc.) without an individual’s consent or knowledge
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The transmission or receipt of computer viruses
- The potential for excessive use which may impact on the social, emotional, development and learning aspects of life

If you find any of these online or discover that someone has been involved in any of them, this constitutes an E-Safety Incident.

A degree of judgement is required on what constitutes an e-safety incident and what is acceptable. Content or communication that may be inappropriate for one student or service user may be acceptable for another. Their age and their ability to process what they are experiencing should be taken into account. Speak to the senior member of staff on site, the E-Safety Champion/Co-ordinator or the IT Manager for further guidance.
4 Preventing E-Safety Incidents

In the ideal world, our aim would be to ensure we don't have any E-Safety Incidents. As we're also trying to encourage our students and service users to be better members of the communities around them, they will have to interact with other people online.

To keep the risks at the absolute minimum, the following steps should always be followed:

- Regardless of the location, staff, students and service users are expected to use Autism Anglia's computers and/or networks with regard to the Acceptable Use Agreements, the IT, Internet and Email Policy and the Data Protection and Confidentiality Policy. Other Support Plans, Care Plans, Education Plans and Risk Assessments may also affect how students and service users may use the computers or other electronic devices.

- Posters and/or leaflets are available near all internet enabled computers belonging to Autism Anglia, to remind all users of the need for diligence and how to report E-Safety incidents.

- Internet Safety Week (first week in February each year) will be on the school calendar and class projects will take place during this time to promote E-safety.

- All Staff will be given easy access to the E-Safety Policy and its importance and application will be explained. Full training on E-Safety will be provided bi-annually, with additional materials supplied to help maintain an up to date awareness.

- The identity of the IT Manager and the relevant E-Safety Co-ordinator/E-Safety Champion will be clearly displayed at each Autism Anglia site.

- Parents/carers will be sent information regarding E-safety through various means, e.g. newsletters, information sheets or dedicated pages on the organisation's web sites. A partnership approach with parents/carers will be encouraged. Parents/carers will be invited to a meeting to be held once a year to provide information on the developments within E-safety.

- School sites have active filtering programs in place, blocking access to sites which contain inappropriate content. The filter in use at the time of writing is fully configurable by IT staff, down to blocking or enabling individual sites for individual users at different times of the day.

- Where filtering programs are in place, these will be monitored regularly for anyone trying to circumvent the system. The monitoring date and any findings will be recorded on the Excel Sheet entitled “E-Safety Incidents”.

- Staff should be aware that no filtering system is capable of accurately filtering every web site. Having a filter in place should not be viewed as a substitute for monitoring the computer activities of students or service users.

- Where filtering systems are not in place, staff should monitor the internet use of Adult Service Users as appropriate, to ensure they adhere to the Acceptable Use Agreements and within the terms of the Data Protection, IT, Internet and Email Policy. However, this monitoring may affect the rights of adult service users to privacy, particularly in their own house or room. Generally speaking, this may mean that only internet use in communal areas or public places may be monitored.

- Staff should be aware that their own internet use may be monitored. Autism Anglia’s IT, Internet and Email policy clearly states that there is no right to privacy with regard to the use of Autism Anglia computers or the use of personal devices on Autism Anglia’s networks. Any deliberate misuse of the systems will be dealt with in accordance with the above mentioned policy.
5 What to Do If You Are Involved in an E-Safety Incident

At Douccroft School, any E-Safety Incidents or misuse of computer systems by students will be managed by representatives from the IT Manager, the E-Safety Co-ordinator, a Designated Person for Safeguarding and members of the Senior Management Team (SMT).

In Adult Services, any E-Safety Incidents or misuse of computer systems by Service Users will be managed by representatives from the IT Manager, a Designated Person for Safeguarding, the relevant Registered Manager, the Regional Manager and the Director of Adult Services.

Those involved in managing the issue must also ensure that the service user, student or staff member receives the necessary support/education following the incident.

A list of Designated Persons for Safeguarding can be found in Section 2.6 and Appendix 1.

5.1 Reporting an E-Safety Incident

E-Safety Incidents fall into 3 categories:
- Staff reporting student or service user
- Student or service user reporting an incident
- Staff reporting another member of staff involved in an incident

Actions taken by staff will be appropriate to which type of incident has happened:
- More serious incidents will be regarded as Safeguarding Issues, e.g. where the individual has been involved in grooming. The safeguarding policies will take precedence over the steps required in this policy.
- Incidents where a staff member has been involved may be considered relevant to the Disciplinary Policy and Procedure.
- Other, more minor incidents, e.g. where the student/service user has accidentally seen an inappropriate web site, will be covered by this policy.

Members of staff encountering an E-Safety Incident must report it to their senior member of staff on site. They in turn will report the incident as appropriate to:
- E-Safety Co-ordinator/E-Safety Champion
- IT manager
- Designated Person for Safeguarding
- Their Senior Manager/Director

5.2 Staff reporting an E-safety Incident involving a Student or Service User

If you discover any of the items listed in Section 3.1 above while online yourself or while supervising a student or service user, your first responsibility is to their safety. Once this is ensured, make full notes of the incident, per the instructions below:

- Firstly, ensure the Student or Service User is no longer at risk by removing them from the situation.
- Make a note of the site and the web address being used and/or which link you clicked when the incident occurred which can be found in the address bar at the top of the screen, where you might expect to see www.google.co.uk or www.autism-anglia.org.uk. It is important to note the full address, so write down everything you see in this box, including any punctuation and symbols.
- Make a record of the date and time of the incident
- Record any names, user names or ‘Avatars’ of those involved
5.3 How Students and Service Users can Report an E-Safety Incident

If a student or service user encounters any of the items listed in Section 3.1 above, they can complete a simpler version of the reporting form, entitled “Student E-Safety Reporting Form” or “Service User E-Safety Reporting Form”. The completed form should be given to a member of staff who will pass it to the E-Safety Co-ordinator/E-Safety Champion.

5.4 Reporting Other Members of Staff Involved in an E-Safety Incident

In the event of a member of staff witnessing or becoming aware of another member of staff causing or otherwise being involved in an e-safety incident, either deliberately or accidentally, this should be reported as a matter of urgency to your Director, Registered Manager, a member of the school’s SMT, a Designated Person for Safeguarding or the IT Manager, using the form entitled “Reporting Staff involved in an E-Safety Incident”. Fill in the form completely with as much information as possible.

Note that failing to report an E-Safety Incident may also result in disciplinary action and, in serious cases, a matter for the police.

5.5 In Each Case

- Ensure you supply as much information as possible, as it may become necessary to report the incident to the police.
- If appropriate, the safeguarding policy/procedure for the locality will be followed.
- The IT Manager or E-Safety Co-ordinator/E-Safety Champion will log the incident, and update it with any outcomes or sanctions.

5.6 What Happens Next?

The senior member of staff on site will need to make an initial judgement on the type of incident, and follow the steps required in other documents as necessary, or as detailed in the sections below.

If you believe the individual concerned has been in contact with an online stranger, the senior member of staff on site should make a report direct to the police via the ‘Click CEOP’ reporting function which can be found at http://ceop.police.uk/safety-centre/

If you believe the individual is in immediate danger, the police should be called directly on 999.

5.6.1 If there has been inappropriate communication or contact

- Report the incident as required in the organisation’s Safeguarding Policy, as a matter of urgency.
- Advise the student, service user or staff member on how to terminate the communication and save all evidence
- The E-Safety Champion/Co-ordinator and/or IT Staff will assist the process by offering help with:
  - Recommending to contact the police using 999 or Click CEOP
  - Logging the incident
  - Identifying suitable support for the student, service user or staff member
5.6.2 If someone has been bullied

- Report to the Senior Manager/IT Manager/E-Safety Co-ordinator/Designated Person for Safeguarding as a matter of urgency.
- Advise the student, service user or staff member not to respond to the message
- Secure and preserve any evidence
- Refer to relevant policies including anti-bullying, e-safety and the acceptable use agreements and apply appropriate sanctions
- The E-Safety Champion/Co-ordinator and/or IT Staff will assist the process by offering help with:
  - Recommending to contact the police using 999 or Click CEOP
  - Logging the incident
  - Identifying suitable support for the student, service user or staff member

5.6.3 If someone has received malicious/threatening comments

- Report to the Senior Manager/IT Manager/E-Safety Co-ordinator/Designated Person for Safeguarding as a matter of urgency.
- Advise the student, service user or staff member not to respond to the message
- Secure and preserve any evidence
- In the case of offending web-based e-mails being received, save a copy of the email in a safe location, away from the person it was sent to.
- The E-Safety Champion/Co-ordinator and/or IT Staff will assist the process by offering help with:
  - Informing the website involved and request that the comments are removed
  - Block further communication from the sender
  - Recommending to contact the police using 999 or Click CEOP
  - Logging the incident
  - Identifying suitable support for the student, service user or staff member

5.6.4 If an illegal website has been viewed (see Section 5.7 below)

- Report to the Senior Manager/IT Manager/E-Safety Co-ordinator/Designated Person for Safeguarding as a matter of urgency
- Do not log off the computer but disconnect the electricity supply from the monitor
- Record the website address as well as the date and time of access
- Refer the student, service user or staff member to the signed Acceptable Use Agreement that was agreed and reinforce the message
- Inform the parent(s)/carer(s) (where appropriate)
- The E-Safety Champion/Co-ordinator and/or IT Staff will assist the process by offering help with:
  - Recommending to contact the police using 999 or Click CEOP
  - Where appropriate, updating the filtering software to prevent any repetition
  - Logging the incident
  - Identifying suitable support for the student, service user or staff member
5.6.5 If an inappropriate website has been viewed (see Section 5.7 below)

- Report to the Senior Manager/IT Manager/E-Safety Co-ordinator/Designated Person for Safeguarding as a matter of urgency.
- Record the website address as well as the date and time of access
- Refer the student, service user or staff member to the signed Acceptable Use Agreement that was agreed and reinforce the message
- The E-Safety Champion/Co-ordinator and/or IT Staff will assist the process by offering help with:
  - Where appropriate, updating the filtering software to prevent any repetition
  - Logging the incident
  - Identifying suitable support for the student, service user or staff member

5.7 Is a site Illegal or Inappropriate?

As a general rule of thumb, if the content of a web site includes material which would be considered illegal in any other medium (printed, television, in person, etc.) then it will be considered illegal content in the UK. For example, images of child abuse, racism, trolling, inciting or extolling violence or other criminal activity, sale of banned or restricted substances, file sharing, copyright infringement, transmission of computer viruses, etc.

Equally, if the content is not illegal by the above definition, it may be considered inappropriate if it would offend some people, not necessarily yourself. This includes offensive, obscene or indecent material including pornography, images of a violent nature, foul or offensive language, etc.
6  Support and Sanctions Following an Incident

Following an E-Safety Incident, the team managing it may offer support to and/or investigate the incident further. Such investigations will be appropriate in cases where an individual’s actions knowingly led to the incident or where there was deliberate misuse.

When managing the conduct of members of staff, breaches of this policy will be investigated according to the organisation’s disciplinary procedures and serious allegations will be treated as gross misconduct.

When considering the options below, support should be offered where possible, with disciplinary action only if deemed necessary. It should be noted that in the case of mainstream school children sending sexualised images of themselves to other students (sexting), the police prefer to educate rather than prosecute, even though possessing any such material is always a criminal offence.

The support available to a staff member, student or service user includes (as appropriate):

-  Counselling
-  Education and Training
-  Specialist support from MDT meetings

The table below shows possible consequences the students at Doucecroft, service users in Adult Services and for Autism Anglia staff:

<table>
<thead>
<tr>
<th>Students at Doucecroft</th>
<th>Service Users in Adult Services</th>
<th>Autism Anglia Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Warning by Class Teacher</td>
<td>• Warning by House Senior</td>
<td>• Warning by Registered Manager/Director/Head Teacher</td>
</tr>
<tr>
<td>• Inform Parents</td>
<td>• Warning by Registered Manager</td>
<td>• Disciplinary action, with the possibility of any outcome including summary dismissal</td>
</tr>
<tr>
<td>• Warning by Senior Management Team</td>
<td>• Removal of internet access for a given period (in accordance with our Deprivation of Liberty Policies)</td>
<td>• Involvement of external agencies, including the police, for serious offences</td>
</tr>
<tr>
<td>• Removal of internet access for a given period</td>
<td>• Involvement of external agencies, including the police, for serious offences</td>
<td></td>
</tr>
<tr>
<td>• Limited network access for a given period</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Involvement of external agencies, including the police, for serious offences</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7  Acceptable Use Agreements

Please refer to separate documents, entitled

- Student ICT Acceptable Use Agreement (for Students at Doucecroft School, including the FE Department)
- Adult Services Service User ICT Acceptable Use Agreement (for Service Users within Autism Anglia Adult Services)
8 Other Resources

There are a range of other organisations, companies and web sites available with resources relating to E-Safety.

If you are caring for or overseeing children or vulnerable adults, it is recommended that you visit these web sites:

CEOP (http://ceop.police.uk/). Run by the police, this site offers advice, resources and a reporting system (available in the top right of the home page).

ThinkUKnow (http://www.thinkuknow.co.uk/). This site is run by CEOP and is presented to engage and educate different age groups, parents/carers and teachers.

Get Safe Online (http://www.getsafeonline.org). A comprehensive range of information, guidance, tips and instructions for staying safe online.

Safe Network (http://www.safenetwork.org.uk/help_and_advice/Pages/safety_online.aspx). Offers practical guidance for organisations helping young people to stay safe online.

ChildNet’s Know IT All (http://www.childnet.com/KIA/). A suite of education resources designed to help educate parents, teachers and young people about safe and positive use of the internet.

Safer Internet Centre (http://www.saferinternet.org.uk/) Tips, advice and resources to help people stay safe online.
## Appendix 1 – Contact Information

<table>
<thead>
<tr>
<th>Post/Role</th>
<th>Post Holder</th>
<th>Base</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustee with responsibility for Safeguarding</td>
<td>Janet Barker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deputy Chief Executive/Overall Safeguarding Lead for Autism Anglia</td>
<td>Alan Bicknell</td>
<td>Head Office</td>
<td>01206 577678</td>
</tr>
<tr>
<td>IT Manager/E-Safety Lead for Autism Anglia</td>
<td>Dan McCullagh</td>
<td>Head Office</td>
<td>01206 577678 or 07719 649009</td>
</tr>
<tr>
<td>Head Teacher/Designated Person for Safeguarding</td>
<td>Jane Smart</td>
<td>Doucecroft School</td>
<td>01206 771234</td>
</tr>
<tr>
<td>Assistant Head Teacher/Designated Person for Safeguarding/E-Safety Co-ordinator</td>
<td>Sam Lawrence</td>
<td>Doucecroft School</td>
<td>01206 771234</td>
</tr>
<tr>
<td>Assistant Head Teacher/Designated Person for Safeguarding/E-Safety Co-ordinator</td>
<td>Kuben Reddy</td>
<td>Doucecroft School</td>
<td>01206 771234</td>
</tr>
<tr>
<td>Care Manager/Designated Person for Safeguarding</td>
<td>Mandy Spragge</td>
<td>Doucecroft School</td>
<td>01206 771234</td>
</tr>
<tr>
<td>Deputy Care Manager/Designated Person for Safeguarding</td>
<td>Jackie Austin</td>
<td>Doucecroft School</td>
<td>01206 771234</td>
</tr>
<tr>
<td>Head of Further Education/Designated Person for Safeguarding</td>
<td>Hayley Fraser</td>
<td>Doucecroft School</td>
<td>01376 570203</td>
</tr>
<tr>
<td>Positive Behaviour Support Manager/Designated Person for Safeguarding</td>
<td>Gayle Jones</td>
<td>Doucecroft School</td>
<td>01206 771234</td>
</tr>
<tr>
<td>Director of Adult Services/Safeguarding Lead/Designated Person for Safeguarding</td>
<td>Angie Steggles</td>
<td>Dereham Office/Head Office</td>
<td>01362 853753/01206 577678</td>
</tr>
<tr>
<td>Essex Adult Services Regional Services Manager/E-Safety Co-ordinator</td>
<td>Hayley Martin</td>
<td>Head Office</td>
<td>01206 577678</td>
</tr>
<tr>
<td>Registered Service Managers</td>
<td>Clare Hanney, Helen Moore, Kim Parsons</td>
<td>Head Office, Peldon Campus, Mersea Road, Supported Living</td>
<td>01206 577678</td>
</tr>
<tr>
<td>IT Instructor/E-Safety Co-ordinator</td>
<td>Matthew Stypulkowski</td>
<td>Jigsaw Study Centre</td>
<td>01206 561877</td>
</tr>
<tr>
<td>Head of Family Support/E-Safety Co-ordinator</td>
<td>Jo Keys</td>
<td>Head Office</td>
<td>01206 577678</td>
</tr>
</tbody>
</table>