Crofton Academy

e-SAFETY Policy

Ref:	Version No:	Date Ratified:	Review Date:
W8	1.0	05.10.21	05.10.24

1. INTRODUCTION

The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. Teachers need to plan to integrate the use of communications technology such as web based resources and email. ICT skills are vital to access life-long learning and employment. Technologies present risks as well as benefits. Internet/social networking use for work, home, social and leisure activities is expanding in all sectors of society. This brings pupils into contact with a wide variety of influences, some of which may be unsuitable. Unmediated internet access through computers, telephones, i-pads etc. brings with it the possibility of placing pupils in embarrassing, inappropriate and even dangerous situations. Refer to Crofton Academy Safeguarding and Child Protection Policy.

2. CORE PRINCIPLES

- Guided Educational Use – curriculum internet use should be planned, task-orientated and educational within a regulated and managed environment.
- Risk Assessment – pupils must be protected from danger (violence, racism, exploitation) and learn how to recognise and avoid it.
- Responsibility – all staff, governors, external providers, parents and pupils must take responsibility for the use of the internet.
- Regulation – in some cases e.g. un-moderated chat rooms, immediate dangers are presented and their use is banned. In most cases strategies on access must be selected and developed to suit the educational activities and their effectiveness monitored.
- This policy is closely related to the guidance contained in: Keeping Children Safe In Education – Statutory Guidance to Schools and colleges (DfE September 2021).
- With regard to radicalisation via the internet and social media the academy fully adopts The Prevent Duty – Departmental Advice for Schools and Childcare Providers (DfE June 2015).

3. USE OF LAPTOPS AND DATA TRANSFERS OFF SITE

- School owned laptops/i-pads/i-phones are provided to a number of staff and/or pupils where it is deemed appropriate that they may need to work on school related matters away from school. This equipment is for the use of members of school staff and/or pupils only.

- Reasonable care is expected to be taken by all members of staff and/or pupils who take such items (e.g. not left in a vehicle overnight).

- Staff are advised not to save personal data on a USB memory stick or external hard drive and consider whether the transfer of personal data is in fact necessary. Staff should consider whether this data is accessible via remote access where it can be accessed and worked on without it leaving the server on which it is stored. Further information is provided in “data in transit” Appendix 1

- Staff should not send emails containing pupil or staff personal data, which if intercepted could be understood and which can identify an individual(s).

4. IMPORTANCE/BENEFITS OF INTERNET USE

- Raise educational standards, promote pupil achievement.
- Support work of staff and enhance management systems.
- Part of the curriculum and a necessary tool in teaching and learning.
- Pupils are entitled to quality Internet access as part of their 21st Century learning experience.
- Access to worldwide resources and experts.
- Educational and cultural exchanges between pupils worldwide.
- Facilitate staff professional development.
- Communication with external services.
- Exchange of curriculum and administrative data/sharing of good practice.

5. ENSURING INTERNET USE ENHANCES LEARNING

- Internet access will be designed expressly for pupil use and will include filtering appropriate to pupils' ages.
- Pupils will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet.
- Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and pupil age.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6. PUPIL EVALUATION OF INTERNET CONTENT

- Any user discovering unsuitable sites must report the address and content to the Network Manager, a teacher or the Designated Safeguarding Lead as appropriate.
- The use of internet derived materials must comply with copyright law.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using internet material in their own work.

7. MANAGEMENT OF EMAIL

- Pupils may only use approved email accounts on the academy system.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication.
- Social email can interfere with learning and will be restricted.
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending.

8. MANAGEMENT OF THE ACADEMY WEBSITE CONTENT

- The point of contact on the website should be the academy address, email and telephone number.
- Staff and pupils' home information will not be published.
- Use of photographs showing pupils and pupils' names will not be used on the website without parental consent.
- The copyright of all material must be held by the academy or be attributed to the owner where permission to reproduce has been obtained.

9. SOCIAL NETWORKING

- Pupils will not be allowed access to public or unregulated chat rooms, social networking sites and forums.
- Pupils may only use regulated chat environments and forums – this use will be supervised, whenever possible, and the importance of chat room safety emphasised.
- In relation to social media staff must:
    - Not accept friendship requests from pupils, past or present (past in this instance means any person who has been taught during a teacher's time at Crofton Academy or any ex-pupil who is under the age of 19 years); and
    - Not approach pupils or family of pupils to be friends, unless they themselves are related or are personal friends of individuals and such on-line friendship will not cause a conflict of interest;
    - Not make disparaging remarks about colleagues, pupils or pupils' family members of the school or be drawn into debate about school related issues in the public domain and remember before they make posts how the world would perceive them if they were viewed by the wider audience and would this be detrimental to themselves and/or the academy;
    - "Untag" themselves if they find themselves tagged in photos they deem to be unsuitable;
    - Ensure that privacy and security settings are set to avoid anyone other than "friends" accessing their accounts or at the very least make their profile not easily identifiable;

- Upload photographs of themselves which include any pupils to social networking sites, even with parental permission, which has not been granted for personal use of photographs by staff (e.g. following a school trip/visit).
- Exercise caution when inviting work colleagues to be "friends" on personal social networking sites. Social networking sites blur the lines between work and personal lives and it may be difficult to maintain professional relationships if too much personal information is known in the work place. It should also be noted that colleagues may have different views as to what is and is not appropriate on line which could lead to conflict.
- Not set up a social media site on behalf of the school; this should only be undertaken by the school under strict instruction to do so.t

10. MANAGING EMERGING TECHNOLOGIES

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

- Mobile phones will not be used during lessons (or on site during the rest of the academy day).

- Where appropriate, the academy's video cameras may be used by pupils for educational use.

11. AUTHORISATION OF INTERNET ACCESS

- All internet access is monitored and recorded using electronic means.

- Inappropriate use of the Internet will be dealt with in accordance with the academy's Behaviour Policy.

12. RISK ASSESSMENT

- Some material available via the internet is unsuitable for pupils. The academy will take all reasonable precautions to ensure such material is not accessed by pupils. However, it is not possible to guarantee that such material will never appear on an academy computer – Crofton Academy cannot accept liability for material accessed or any consequences of internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

- Methods to identify, assess and minimise risk will be reviewed regularly.

13. MANAGEMENT OF FILTERING

- The academy will work in partnership with parents/carers, the DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

- Any internet user must report unsuitable/illegal sites to the class teacher, ICT Technician (and the Designated Safeguarding Lead if necessary) immediately. s

- The ICT Technician will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is filtered and communications are monitored.

- If filtered websites need to be used by staff, they must inform ICT Technician to have them unblocked for a set period of time (requests need to be approved by the Line Manager).

14. ICT SYSTEM SECURITY

- The academy's ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Files held on the academy's network will be regularly checked.
- Use of portable media such as memory sticks and CD will be reviewed regularly.
- Downloading of unauthorised files will be prohibited, and where possible blocked.
- Use of the academy's ICT systems will be subject to GDPR, Data Protection Act and the Computer Misuse Act.

15. PUPIL, STAFF AND PARENTAL AWARENESS

- All stakeholders will be made aware of this policy and how it relates to them.
- Pupils will be instructed in responsible and safe internet use before being granted access.
- Responsible use of the internet, including social networking will be discussed through the Computing curriculum, assemblies and Personal Development Programme.
- The monitoring of internet use is a sensitive matter – staff who operate monitoring procedures will be supported by the Network Manager and responsible Assistant Headteacher.
- Staff training in safe and responsible internet use and on the contents of this policy will be provided as required.
- A partnership approach with parents/carers will be encouraged, with relevant information on issues covered by this policy made available.
- Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the academy's Behaviour, Anti-Bullying and Safeguarding and Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel.

APPENDIX 1

DATA IN TRANSIT

DATA AND THE LAW

The Data Protection Act 1998 requires all data controllers (in this instance "the School") and those within the organisation to use data responsibly with due care to security. The School has a Privacy Notice which is issued to all parents/carers outlining what the data we collect is used for and who it may be shared with.

Members of staff have access to some data and may well need it for day to day activities. As some staff work at home as well as school, care needs to be taken with regard to data being taken offsite. **Staff could be held liable for data that they do not take reasonable care of whether it is in electronic form or hard copy.**

USB AND MEMORY STICKS

The school acknowledges that staff use USB memory sticks. These are a common and convenient way of transporting data. **We strongly recommend that any pupil data is held only on hardware encrypted USB sticks with 128 bit encryption.**

These devices require an access code and some securely delete the information they contain if this passcode is entered incorrectly more than a specified number of times.

Staff should consider, when transferring data onto a USB memory stick, whether it needs to be transferred at all. Can the data be saved onto a school laptop? We do not expect or allow members of staff to download confidential information to private homes PCs or laptops. School reminds staff that laptops loaned to them are for their use only and are not for use by other member of their family thereby allowing others to potentially access confidential data. **Staff are responsible for what others do on these laptops.**

LOSS OF DATA

Staff should be aware that they are personally responsible and liable for loss of data. The data owner is the pupil, parent/carer, fellow member of staff to whom the data relates, and they may have a claim against a member of staff who has lost their confidential data if they have not taken reasonable care of it, and the pupil, parent/carer, or fellow member of staff have been harmed as a result.

Whilst we appreciate staff may need to work with personal data on children, we invite you to consider better ways of working for example considering whether this data is accessible via remote access where it can be accessed and worked on without it leaving the server on which it is stored.

If you lose a USB memory stick that has confidential information on it, in some instances this may be sensitive personal data, you should report this to the Headteacher immediately.