3.2 IT and Communications Policy

Relevant Chapter

Policy

We propose to make the most of the advantages offered by modern electronic communication. All computers provided are primarily for business use. Limited personal use of the computer system is permitted if it does not interfere with an individual's or other employee's work performance and complies with security and use guidelines set out in this document.

There are 4 main laws which have been taken into consideration when developing our communications policy:

i. The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas

ii. Human Rights Act 1998 - gives individuals the right to privacy;

iii. Lawful Business Practice Regulations - gives employers the lawful authority to intercept communications in controlled circumstances;

iv. Lawful Business Practice Regulations - gives employers the lawful authority to intercept communications in controlled circumstances;

Any problems occurring from any misuse of company computers may result in staff or YPs being charged for any repairs or maintenance that may be needed or the need for disciplinary or grievance proceedings.

Contents

1 Legislative Framework

England

- Regulation 22: Contact and access to communications
- Regulation 38: Storage of records, etc.
- Regulation 12: The protection of children standard

  http://www.legislation.gov.uk/uksi/2015/541/regulation/12/made
- General data protection rules (GDPR)

Wales

- Regulation 26: Safeguarding – overarching requirement https://www.legislation.gov.uk/wsi/2017/1264/regulation/26/made
- Regulation 27: Safeguarding policies and procedures https://www.legislation.gov.uk/wsi/2017/1264/regulation/27/made
- Regulation 48: Facilities and equipment https://www.legislation.gov.uk/wsi/2017/1264/regulation/48/made

2 Outcome

Employees will understand how to use and apply technology safely, both, in the work place and within personal circumstances. Young people will learn how to use technology safely and with appropriate supervision.

3 Aims

This guidance aims to:

a. Ensure safeguarding children/young people in the digital world is a priority;
b. Assist employees to work safely and responsibly within a framework of best practice;
c. Set down the standards of behaviour that the company expects from its employees;
d. Minimise the risk of allegations being made against employees about inappropriate behaviour;
e. Project a clear message that unlawful or unsafe behaviour is not acceptable; (f) Establishes a culture that safeguards children/young people and company employees.
f. Using technology to facilitate 'every day communication' is now the 'norm' for most employees and children/young people. However, within this scenario the practitioner will have a dual 'persona' if you will. An electronic self that is personal and an electronic self that is 'at work'.
g. This guidance sets down the standards of behaviour that are expected from the 'at work' persona and gives advice on how to keep the personal private. Any breaches of this guidance could result in an employee being referred to the disciplinary procedure.

4 Online safety procedure

1. All staff will have regard to the organisation’s online safety and safer use of technology policy.
2. Managers will ensure that all staff are aware of the policy and how it applies in the home and in regard to their professional conduct.

3. Managers will ensure that all staff skilled in helping young people to use the internet safely.
4. Managers will ensure that all staff are also aware of the Online Child Abuse and Exploitation policy and the reporting arrangements for all safeguarding concerns.
5. All young people will have an internet access risk assessment and permissions sought from social workers for young people to use the Internet.
6. All young people's access and use will differ based on their individual risk assessment. For this reason, all young people should have an individual acceptable use agreement. This should be drawn up with the young person and agreed with their social worker.
7. An agreement might include;
    a. Time limits.
    b. The type of sites or specific sites that the young person is permitted or not permitted to use.
    c. Agreement to explain or show staff what they are doing online at any time.
    d. Any behaviour that is unacceptable e.g. bullying, gossiping, sharing sexual images.
    e. If the young person accesses social networking sites, agreement to share who their online 'friends' are, ensure privacy settings are appropriately set and establish the type of activity that is acceptable;
    f. The need to tell someone if inappropriate content is accessed or they are upset by anyone while online;
    g. The need to ask before carrying out certain activities e.g.: setting up an account on a games site, joining a social networking site.
    h. The consequences of not following the agreement.

8. The manager must ensure that boundaries and rules around the times the internet can be used are consistently followed and that young people are not online after the approved times or when they are supposed to be sleeping.

9. Young people not in education should not be accessing the Internet during the school day other than for education-related activities and must be supported by staff.

10. All young people will have reasonable access to send and receive electronic mail in private however Internet security must be set on all computers used in the home including young people's personal laptops where applicable.

11. Disabled young people will be provided access to such aids and equipment they might need dependent on their communication needs, to access electronic communications.

12. All young people will receive age-appropriate safe use education including issues around sexting, online pornography, online gaming and cyberbullying. Managers will need to ensure staff are aware of what education young people receive in school and if education is provided at the home, lessons should include online safety.

13. Managers will ensure the staff team are aware of the dangers young people face online including online grooming, cyberbullying, exploitation, inappropriate contents, messaging and friend applications and how to promote social networking safely. Reference must be made to related safeguarding policies.

14. Managers must ensure there is good awareness in the team as to the signs that young people may be in danger of online exploitation. Such as too much time online, secrecy around their phones or computers or changes in behaviour that may indicate stressful experiences.

15. Managers must ensure young people are educated on safe digital footprints, the dangers of

sending personal information, photos and agreeing to meet people met on the internet?

16. Managers must ensure young people receive guidance on safe internet use, cyberbullying and signposts to who young people can talk to if they have concerns.

17. The manager must ensure internet use is subject to privacy settings and monitoring mechanisms to ensure the internet is being used safely.

5 The Work Environment

5.1 Access to Communications

1. The registered manager/home manager must ensure that children/young people are provided at all reasonable times with access to the following facilities which they may use without reference to persons working in the home:
   (a) A telephone on which to make and receive telephone calls in private; and
   (b) Facilities to send and receive post and, if the necessary facilities are provided for the use of children/young people, electronic mail, in private.
2. The registered manager/home manager must ensure that a disabled child/young person accommodated in the home is provided with access to such aids and equipment as he/she may require as a result of their disability in order to facilitate the child's/young person's communication with other persons.
3. If the registered manager/home manager considers it to be necessary for the purpose of safeguarding or promoting the welfare of a child/young person, they may impose conditions, prohibitions or restrictions upon a child's/young person's access to communications.
4. Only equipment owned and certified by the Company must be used to facilitate the young people's communication needs. Staff must never give or lend personal equipment to young person in their care. (Mobile phones, tablets, laptops or any other personal device). As a safeguarding measure and to save confusion staff must ensure that any personal devices are locked away whilst on shift and only use the communication devices provided by the company. Not following this management instruction could result in disciplinary action. If proven such a breech is deemed as gross misconduct.

5.2 Using Email, Mobile Phones, Instant Messaging and Social Networking Sites

The following points must be adhered to when using information communication technology:

1. Only use devices contracted to / provided by the company e.g. mobile phones, office phones, PCs.

NEVER USE, GIVE or LEND ANY PERSONAL DEVICES.

2. Only use email addresses, instant messaging identities or social networking accounts that have been formally established and approved by the company for professional purposes;
3. Staff should not have online communication with children/young people, should not share their email addresses or 'link' with children/young people through social networking sites;
4. Employees must be careful not to take risks in their communications with children/young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be interpreted as grooming;

5. Your personal e-mail addresses, instant messaging identities, social networking accounts or home/mobile telephone accounts must not be used to contact children/young people;
6. Employees should be aware of and comply with company policy on the use of email, text and instant messaging;
7. Take care when establishing user names and automatic signatures to ensure that they are appropriate for communicating in a professional setting;
8. We recognise that text communication can be a quick and simple way of communicating, however staff must give thought to the appropriateness and context of any communication method;
9. Staff should avoid using text messages for formal communication at work. For example, it is not appropriate to contact a manager to advise of sickness absence using text. A personal telephone call is required.

5.3 Using Social Networking Sites as a Source of Information

1. Social networking sites can also be used to obtain valuable information about a person's contacts and activities. Where a member of a social networking site has not used the site's security and privacy settings, to restrict visibility of the information associated with their profile, then that information is openly available in the public domain. It is therefore available for others to view and use without restriction.
2. Social networking sites can be used forensically to help provide more information in certain situations.
3. Increasingly, staff will use social networking sites in their personal lives and as a result will be 'linked' to other work colleagues. Staff must take personal responsibility for their boundaries and communication outside work. Under no circumstances should you post any comments or information relating to your work, the organisation or work colleagues.
4. Staff should also be aware and sensitive to personal information about themselves that they (or others) may post which may bring conduct, behaviour or judgement into question.

5.4 Photographing and Video

There are many situations where it is normal for employees, children/young people to take photos or make a video to record an event e.g. birthdays, holidays, school and sporting events. This should be encouraged; however, there are potential dangers. Staff must not use personal cameras and mobile phones and use company equipment instead. One potential danger is an allegation that an employee has taken an inappropriate photo. With a personal camera it would be more difficult for the employee to prove that this was not the case. With company equipment there is at least a demonstration that the photography was consistent with company policy. In all instances where the employee undertakes photography it must be recorded.

5.5 Issues of Consent

1. Photographers must ask for permission to take a photo to ensure compliance with the General Data Protection Regulation (GDPR). This is because an image of a child/young person is personal data for the purpose of the Act and it is a requirement that consent is obtained at referral from the parent, carer, guardian or corporate parent of the child/young people under the age of 18 years (or the child him or herself if deemed competent from 12 years old as suggested by the Information Commissioner) for any photographs or video recordings for purposes beyond a school's core educational function. It is also important to ascertain the views of the child/young person. Parents retain the right to withdraw consent at any stage and this must be made in

writing. In each case the consent of the line manager must be given and recorded before taking images or videos of children/young people.

2. There will be many situations such as adoption placement or resettlement from domestic violence where a child's/young person's security is known to be at stake indicating the need for extra care where photography/video could end up on display.

5.6 Storage

The registered manager/home manager must ensure that the following items, which may be kept in electronic form, are kept in an accessible manner:

5.7 Other Records such as Photos and Videos

1. Care must also be taken that photos and video are stored appropriately. For instance, to copy the images onto a personal PC as opposed to a work allocated PC might make it difficult to retain control of how a picture is used or who has access to it. Secure memory cards, memory sticks and CDs provided by work must only provide a temporary storage medium. Once the images have been uploaded to the appropriate area of the company's network, those images must be erased immediately from their initial storage location.
2. It is not appropriate to amend or manipulate images (exceptions may be to brush out anything that can identify where a child/young person lives or which school they attend or to crop a picture to fit).

6 Personal Environment

6.1 Keeping Safe

1. Employees working with children/young people must take extra care in establishing, managing and using their profiles on social networking sites. Strong passwords should be used and security and privacy settings should regularly re-applied so that you can control all access to your profile and any personal information that you publish.
2. Once 'out there' published, personal information such as photos and blog posts can be impossible to control and could potentially be manipulated without your consent or knowledge, used in different context or distributed. Joining specific online games or Facebook groups could also be misinterpreted. A good guideline is only publish content that you would be happy to share with your employer.
3. False social networking profiles can be set up by children/young people, parents / carers and even colleagues to spread false or malicious information about employees. Few social networking sites authenticate their members offline and, generally, they use automated registration systems which can only provide limited checks. You need to know who you are talking to online, people are not always who they say they are.
4. The use of social networking and instant messaging is often conversational with a rapid interchange of remarks. It is easy to stray from a non-work conversation between friends to professional matters which could be seen as a breach of professional confidentiality. Employees should either be fully conversant with the security and privacy setting for the site in use or should avoid posting any information that could compromise their professional integrity.
5. Individual social networking sites publish their own guidelines on how to manage privacy settings and restrict visibility from other web users. It is recommended that these are accessed and used on a regular basis to prevent your private information and comments becoming published in the public domain and available to all including other employees of the company.

6. There are a range of offences regarding the incitement of hate, harm and harassment on the basis of race, religion and sexual orientation. The harassment or threatening of individuals includes cyberbullying by mobile phone, social networking sites etc. It is an offence to send indecent, offensive or threatening messages with the purpose of causing the recipient distress or anxiety.

6.2 Behaviour on the Web

6.2.1 Inappropriate Behaviour

Think about this in respect of professionalism and being a role model. The scope here is enormous bearing in mind that actions outside of the workplace could be considered a fundamental breach of trust and confidence placed in the employee and may constitute gross misconduct. Examples include:

1. Posting offensive or insulting comments about the company;
2. Accessing adult pornography on work computers;
3. Making derogatory comments about children/young people or colleagues on social networking sites;
4. Trading in sexual aids, fetish equipment or adult pornography.

6.2.2 Inappropriate Material

Inappropriate is a term that can mean different things to different people. It is important to differentiate between 'inappropriate and illegal' and 'inappropriate but legal'. All employees need to be aware that in the former case investigation may lead to criminal investigation, prosecution, dismissal and barring. In the latter it can still lead to disciplinary action, dismissal and barring even if there is no criminal prosecution.

6.2.3 Illegal Material

1. Accessing (viewing) making, storing (possessing) or disseminating indecent images of children/young people on or off the Internet, whether on or off work premises is illegal. If proven this will lead to criminal proceedings and the individual will be barred from working with children/young people.
2. Sharing adult pornography with children/young people is illegal.
3. Possessing or distributing indecent images of a person under 18 can include viewing such images online. This may also constitute possession even if they are not saved.
4. For more information and guidance you can contact your Local Safeguarding Children’s Board.

7 Guidance for Internet Security Breaches

1. Whilst the internet can provide invaluable resources it must also be acknowledged that the security of data and the physical and emotional safety of children/young people can be inadvertently compromised.
2. Parental restrictions, firewalls and other security measures are all capable of

1. Being overridden particularly with multiuser environments and, as such, cannot be guaranteed to provide complete safety.
2. Even with updated measures staff must be aware of recent cases of cyber blackmail (amongst

other scams) in which criminals threaten to download images of child pornography unless a 'ransom' is paid.

3. Accordingly, all computers maintained at the company's registered homes have systems that prohibit access to Internet browsing and restrict usage to the transmission of email only.
4. The exception to this rule is for computers used exclusively by education staff who are issued with laptop computers for use during 1:1 sessions with child/young person.
5. During educational sessions any internet use is closely supervised by education staff and the laptops are removed from registered homes after use.
6. Education laptops are regularly inspected by our IT support consultants to ensure that security has not been compromised. In certain circumstances and subject to risk assessment children/young people may use the local authority lending library facilities to access Internet services.
7. Children's Services do not allow Internet browsing. Any attempts by users to circumvent the security measures will result in immediate disciplinary action.
8. All users must report any breaches in security immediately e.g. ability to access browsing, pornographic images downloaded or forming email attachments, cyber threats, hacking etc.

8 Revision History

Date last updated: May 2020

Date of next review: May 2021

Date of release: December 2018

End