Data Protection: Rights and Obligations NEU guidance for members in England & Wales

The purpose of this document is to provide a broad outline of rights and responsibilities under data protection legislation.

What are the General Data Protection Regulations?
The General Data Protection Regulations (GDPR) came into force in May 2018 and (together with the Data Protection Act 2018) replace the Data Protection Act 1998. They set out rights of individuals (such as employees and students) and the obligations of employers and organisations (such as schools and local authorities) in relation to personal information.
The GDPR set out six principles that data controllers (such as schools, colleges, universities and local authorities) should follow when using personal information (eg collecting, storing, retrieving, disclosing or destroying this information).
These include:
• the obligations to process personal data lawfully, fairly and in a transparent manner
• only to collect data for specified, explicit and legitimate purposes
• to keep personal information accurate and, where necessary, up to date
• to keep personal information secure.
The GDPR also provides for individuals' right of access to personal data held about them.
The Information Commissioner's Office (ICO) produces helpful guidance on data protection issues, including a code of practice on these issues in the workplace.

Can I obtain my personal information?
The GDPR gives you the right (subject to some exceptions) to see most personal information held about you by your employer, businesses and organisations in the public and private sectors. The right to access is set out in article 15 of the GDPR and (usually) must be provided free of charge.

How do I make a request?
You need to make a written request to the ‘data controller’, ie the person/organisation who holds personal information about you. For example, your employer is a data controller.

Can my request be refused?
An organisation may refuse your subject access request if your data includes information about another individual, except where:
• the other individual has agreed to the disclosure, or

• it is reasonable to provide you with this information without the other individual's consent.
In deciding this, the organisation will have to balance your right to access your data against the other individual's rights regarding their own information.
The organisation can also refuse your request if it is considered 'manifestly unfounded or excessive'.
In any case the organisation will need to tell you and justify its decision. It should also let you know about your right to complain to the ICO, or through the courts.

Can I get information about other people and can they get information about me?
You can only access other people's personal information if you are acting on their behalf and if they have given their permission to the employer for the information to be disclosed to you. This means that your employer may not discuss your concerns with your spouse, partner, friend or trade union representative until you give permission.
Similarly, other people can only access your information if they are acting on your behalf and you have given your permission to the employer for the information to be disclosed to them.

Can information about me be used or disclosed without my consent?
As stated above, data must be processed lawfully under the GDPR. The 'data subject' can give consent to the processing of their data and that is a lawful basis. Consent must be given by a "clear and affirmative act". This means that the individual must opt in to consent, rather than opt out. Consent can also be withdrawn at any time.
A data controller can rely on other lawful reasons for processing data, such as:
• that processing the data is necessary for the performance of a contract which the data subject is a party to
• processing is necessary for the purposes of the legitimate interests pursued by the data controller
• that it is necessary for compliance with a legal obligation.
Except in exceptional circumstances, such as a police investigation, the general rule is that you should be aware that personal data about you has been, or is going to be, shared with others, even if your consent to such sharing is not needed.

Can my manager publish my sick record?
Your employer can publish totals of sickness absence as long as individual employees are not identifiable.
The Information Commissioner's Employment Practices Data Protection code seeks to ensure that managers have access to no more information about their workers' health than they are likely to need. However, a manager's concern should primarily be with the impact of a medical condition on a worker's fitness for work, rather than with the medical details.

Do I have a right to see emails about me?
You may be entitled to make a data subject access request for copies of emails held about you. For information to fall within the GDPR subject access provisions, you have to be identifiable from the data and it must relate to you. This means, for example, that an email about your conduct or performance will almost certainly have to be provided. However, an email that simply mentions you as your name appears on the email address list may not have to be provided.

How long can my employer keep information about me?

There is no specific period given in the GDPR. It is left to the employer to set retention periods. The GDPR requires that the personal information in a record should not be kept for longer than is necessary for a particular purpose or purposes.
As far as possible, standard retention times should be set out in a school/local authority/college policy. There may also be other statutory requirements to retain records such as tax records and health and safety records.

Do I have a right to see the notes made about me at interview?
There is no general exemption from the GDPR's subject access rights in respect of interview notes about candidates. This means that when an individual makes a request for access to the notes, it should be granted in most cases.

Do I have a right to see the reference issued by my employer?
You do not have an automatic right to see references provided in confidence, although some employers work on the basis that it is good practice to share the content of references with employees before sending them. After all, nothing within the reference should be unexpected. If your employer will not provide you with a copy of the reference, you may request a copy from the employer to whom the reference was sent. If you make a request for a reference from the supplying employer, they can refuse as there is an exemption under the GDPR in relation to job references.
You should write to the prospective employer requesting access to the information that they hold about you.

Can employees' personal messages be monitored by employers?
Yes, if the equipment being monitored belongs to the employer. In a landmark 2016 judgement, the European Court of Human Rights (ECHR) ruled that private communications sent during work hours from company devices can be accessed by employers, where there are reasonable grounds for doing so. Romanian Bogdan Barbulescu had been told by his employer to set up a Yahoo Messenger account to deal with enquiries from clients. When his employer accused him of using it for his own ends in office hours, he denied it – but was presented with a 45-page dossier of his private correspondence.
Mr Barbulescu challenged his sacking in Romania's courts and – after losing his case – appealed to the ECHR. His claim that his right to privacy had been breached was rejected by the judges. Their ruling said: "It is not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours." The decision affects all the countries that have signed up to the ECHR, including Britain.
The NEU believes employers should ensure their IT policies provide clear, unambiguous guidance about the monitoring of staff members' emails. The union advises members to ensure that all communications sent during work hours from company devices are entirely professional.

What if my employer reads my personal messages without good reason?
It is a very serious offence for managers to engage in such practices, even if the personal messages appear on equipment belonging to the employer, and particularly where the employer permits a limited amount of personal use. Employers are not free to 'phish' for information simply to see what may turn up. The union's advice is not to use your employer's networks to communicate with the union or with colleagues in a non-work capacity. If you do, because it is convenient to do so, contact the union as soon as possible if you have reason to believe that your messages are being opened and read covertly, and without good cause.

Can we publish our students' examination results?
Publishing examination results constitutes processing personal information and so falls under the terms of the GDPR. Any educational institution wishing to publish exam results must therefore ensure they comply with the six principles under the GDPR:

- **Lawfulness, fairness and transparency** - you must process personal data lawfully, fairly and in a transparent manner in relation to the data subject.
- **Purpose limitation** - you must only collect personal data for a specific, explicit and legitimate purpose. You must clearly state what this purpose is, and only collect data for as long as necessary to complete that purpose.
- **Data minimisation** - you must ensure that personal data you process is adequate, relevant and limited to what is necessary in relation to your processing purpose.
- **Accuracy** - you must take every reasonable step to update or remove data that is inaccurate or incomplete. Individuals have the right to request that you erase or rectify erroneous data that relates to them, and you must do so within a month.
- **Storage limitation** - You must delete personal data when you no longer need it. The timescales in most cases aren't set. They will depend on your business' circumstances and the reasons why you collect this data.
- **Integrity and confidentiality** - You must keep personal data safe and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In particular, they must ensure publication is fair and lawful. Pupils and parents should be informed that publication will take place and should be given information about the format of the publishing.
This might include the name of the publication in which the results will appear, when they will be published and whether the results will be listed by grade or in alphabetical order of entrant name. Where publishing results may cause distress or harm, serious consideration should be given to any objections, and the results should only be published if there is a justifiable reason to proceed.
Information relating to examination results held by educational institutions is likely to be personal data as defined under the GDPR. Therefore, students have a right to access some of this data.
You may have come across situations where students have asked for copies of exam scripts, examiners' comments and marks. There is an exemption under the GDPR so that students do not have the right to see examination scripts or the information recorded in them.
However, examiners' comments fall outside this exemption. If an examiner recorded comments about a particular candidate in a margin or on a separate sheet, this would probably be personal data and the student would have a right to see the comments.
There is also a provision under the GDPR for educational institutions to delay giving a response to a data access request where the request to see exam marks has been made before the results are announced.

Can we take and keep biometric information?
Many schools use biometric data, for example, using fingerprints as a means of accessing school dinners rather than paying by cash. Parents/carers must be notified of any biometric recognition system before it is put in place or before their child first takes

part in it. Pupils and parents/carers also have the right to choose not to use a biometric system, and an alternative means of accessing the service must be available. The information must only be used for the purpose for which it is collected. The same rules also apply to members of staff if biometric data is collected from them.

Are photographs personal data?
There are many circumstances in which people may want to take photographs in schools, for example, by parents at sports days, plays and other school events. Staff may want to take photos for the school prospectus or website. Where photographs are for personal use, there are no data protection implications. Therefore, there is no reason to prevent parents from taking photographs in the situations mentioned above, provided they are for personal use such as placing in a family album.
However, where photos are taken for official use (for school/college business), some of these photographs are personal data as defined under the GDPR, and must therefore be processed lawfully, fairly and transparently. For example, photographs taken for security identification passes and stored on a computer along with other information about the individual are personal data, and the GDPR applies. It would therefore be sensible to consult with pupils and/or guardians before taking such photos.
The media should also seek the consent of the school/college and pupils and/or their guardians before publishing photographs of pupils. If your photo is taken for security purposes, it should not be used for other reasons without your explicit consent. Your photograph should certainly not appear on a school/college website or prospectus without your knowledge and consent.

Can I take students' work home to mark?
Yes. You should be careful where you store it to ensure members of your household and visitors to your home cannot access it, but otherwise it is important that a common sense approach is adopted around the GDPR to ensure people can still perform their job effectively. If you use devices or software outside of your employer's premises, they must ensure you are secure.

What should I do next?
If further advice is needed, contact your NEU workplace rep in the first instance. If there is no NEU rep in your workplace, or the peripatetic nature of your employment makes contact with a workplace rep difficult, contact the NEU Adviceline in England on 0345 811 8111 or NEU Cymru in Wales on 029 2046 5000.
Further contact details may be found at: neu.org.uk/contact-us

Further information
The Information Commissioner
ico.org.uk